ISG50

Integrated Service Gateway

User's Guide

ZyXEL
ISG50

ZyXEL
ISG50

Default Login Details

LAN IP Address	https://192.168.1.1
User Name	admin
Password	1234

Version 2.30
Edition 3, 05/2012

ZyXEL

www.zyxel.com

Copyright © 2012
ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to show you how to make the ISG50 hardware connections and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a connection diagram and package contents list.

- CLI Reference Guide

  The CLI Reference Guide explains how to use the Command-Line Interface (CLI) to configure the ISG50.

Note: It is recommended you use the Web Configurator to configure the ISG50.

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

-

How To Use This Guide

- Read Chapter 1 on page 27 chapter for an overview of features available on the ISG50.
- Read Chapter 3 on page 43 for web browser requirements and an introduction to the main components, icons and menus in the ISG50 Web Configurator.
- Read Chapter 4 on page 59 if you're using the installation wizard for first time setup and you want more detailed information than what the real time online help provides.
- Read Chapter 5 on page 69 if you're using the quick setup wizards and you want more detailed information than what the real time online help provides.
- It is highly recommended you read Chapter 6 on page 87 for detailed information on essential terms used in the ISG50, what prerequisites are needed to configure a feature and how to use that feature.
- It is highly recommended you read Chapter 7 on page 107 for ISG50 application examples.
- Subsequent chapters are arranged by menu item as defined in the Web Configurator. Read each chapter carefully for detailed information on that menu item.
- To find specific information in this guide, use the **Contents Overview**, the **Table of Contents**, the **Index**, or search the PDF file.

Contents Overview

User's Guide 25

Introducing the ISG50 27
Features and Applications 37
Web Configurator 43
Installation Setup Wizard 59
Quick Setup 69
Configuration Basics 87
General Tutorials 107
PBX Tutorials 135

Technical Reference 183

Dashboard 185
Monitor 195
Registration 229
Interfaces 233
Trunks 281
Policy and Static Routes 289
Routing Protocols 302
Zones 313
DDNS 317
NAT 323
HTTP Redirect 331
ALG 335
IP/MAC Binding 341
Authentication Policy 347
Firewall 353
IPSec VPN 367
Bandwidth Management 397
ADP 411
Global PBX Settings 429
Voice Interfaces 448
Extension Management 453
Outbound Trunk Group 477
Auto-attendant 503
LCR 519
Group Management 526
Call Services 532
Call Recording 544

Meet-me Conference 547
Paging Group 549
ACD 553
Sound Files 568
Auto Provision 573
Voice Mail 581
Phonebook 587
Office Hours 595
User/Group 599
Addresses 613
Services 619
Schedules 625
AAA Server 631
Authentication Method 639
Certificates 643
ISP Accounts 661
System 665
Log and Report 705
Call Detail Record (CDR) 720
File Manager 725
Diagnostics 737
Packet Flow Explore 745
Reboot 753
Shutdown 755
Extension Portal 757
Troubleshooting 765

Table of Contents

Contents Overview 3

Table of Contents 5

Part I: User's Guide 25

Chapter 1
Introducing the ISG50 27

1.1 Overview 27
  1.1.1 PBX 27
  1.1.2 Security and Routing 28
  1.1.3 Application Scenarios 28
1.2 Rack-mounted Installation 31
  1.2.1 Rack-Mounted Installation Procedure 32
1.3 Connecting the Frame Ground 32
1.4 Front Panel 33
  1.4.1 Front Panel LEDs 33
1.5 3G PCMCIA Card Installation 34
1.6 Management Overview 34
1.7 Starting and Stopping the ISG50 35

Chapter 2
Features and Applications...37

2.1 Features 37

Chapter 3
Web Configurator...43

3.1 Web Configurator Requirements 43
3.2 Web Configurator Access 43
3.3 Web Configurator Screens Overview 45
  3.3.1 Title Bar 45
  3.3.2 Navigation Panel 46
  3.3.3 Main Window 52
  3.3.4 Tables and Lists 54

Chapter 4
Installation Setup Wizard 59

4.1 Installation Setup Wizard Screens 59

4.1.1 Internet Access Setup - WAN Interface 59
4.1.2 Internet Access: Ethernet 60
4.1.3 Internet Access: PPPoE 62
4.1.4 Internet Access: PPTP 63
4.1.5 ISP Parameters 63
4.1.6 Internet Access Setup - Second WAN Interface 65
4.1.7 Internet Access - Finish 66
4.2 Device Registration 66

Chapter 5
Quick Setup....................69

5.1 Quick Setup Overview 69
5.2 WAN Interface Quick Setup 70
5.2.1 Choose an Ethernet Interface 70
5.2.2 Select WAN Type 71
5.2.3 Configure WAN Settings 72
5.2.4 WAN and ISP Connection Settings 72
5.2.5 Quick Setup Interface Wizard: Summary 75
5.3 VPN Quick Setup 76
5.4 VPN Setup Wizard: Wizard Type 77
5.5 VPN Express Wizard - Scenario 78
5.5.1 VPN Express Wizard - Configuration 79
5.5.2 VPN Express Wizard - Summary 80
5.5.3 VPN Express Wizard - Finish 81
5.5.4 VPN Advanced Wizard - Scenario 82
5.5.5 VPN Advanced Wizard - Phase 1 Settings 83
5.5.6 VPN Advanced Wizard - Phase 2 84
5.5.7 VPN Advanced Wizard - Summary 85
5.5.8 VPN Advanced Wizard - Finish 86

Chapter 6
Configuration Basics....................87

6.1 PBX Features Overview 87
6.1.1 Call Routing 87
6.1.2 Internal Call Routing 89
6.1.3 Outbound Call Routing 89
6.2 Object-based Configuration 91
6.3 Zones, Interfaces, and Physical Ports 92
6.3.1 Interface Types 92
6.3.2 Default Interface and Zone Configuration 93
6.4 Terminology in the ISG50 94
6.5 Packet Flow 94
6.5.1 Routing Table Checking Flow 95

6.5.2 NAT Table Checking Flow 96
6.6 Other Features Configuration Overview 97
6.6.1 Feature 97
6.6.2 Licensing Registration 98
6.6.3 Interface 98
6.6.4 Trunks 98
6.6.5 Policy Routes 98
6.6.6 Static Routes 99
6.6.7 Zones 99
6.6.8 DDNS 100
6.6.9 NAT 100
6.6.10 HTTP Redirect 101
6.6.11 ALG 101
6.6.12 Auth. Policy 101
6.6.13 Firewall 101
6.6.14 IPSec VPN 102
6.6.15 Bandwidth Management 102
6.6.16 ADP 103
6.7 Objects 103
6.7.1 User/Group 104
6.8 System 104
6.8.1 DNS, WWW, SSH, TELNET, FTP, SNMP 104
6.8.2 Logs and Reports 105
6.8.3 File Manager 105
6.8.4 Diagnostics 105
6.8.5 Shutdown 105

Chapter 7
General Tutorials 107

7.1 How to Configure Interfaces, Port Roles, and Zones 107
7.1.1 Configure a WAN Ethernet Interface 108
7.1.2 Configure Port Roles 108
7.1.3 Configure Zones 108
7.2 How to Configure a Cellular Interface 109
7.3 How to Configure Load Balancing 111
7.3.1 Set Up Available Bandwidth on Ethernet Interfaces 111
7.3.2 Configure the WAN Trunk 112
7.4 How to Set Up an IPSec VPN Tunnel 113
7.4.1 Set Up the VPN Gateway 114
7.4.2 Set Up the VPN Connection 115
7.4.3 Configure Security Policies for the VPN Tunnel 116
7.5 How to Configure User-aware Access Control 116
7.5.1 Set Up User Accounts 117

7.5.2 Set Up User Groups 118
7.5.3 Set Up User Authentication Using the RADIUS Server 118
7.6 How to Use a RADIUS Server to Authenticate User Accounts Based on Groups 120
7.7 How to Use Authentication Policies 122
7.7.1 Configure the Authentication Policy 122
7.8 How to Configure Service Control 123
7.8.1 Allow HTTPS Administrator Access Only From the LAN 123
7.9 How to Allow Incoming H.323 Peer-to-peer Calls 125
7.9.1 Turn On the ALG 126
7.9.2 Set Up a NAT Policy For H.323 126
7.9.3 Set Up a Firewall Rule For H.323 128
7.10 How to Allow Public Access to a Web Server 129
7.10.1 Create the Address Objects 129
7.10.2 Configure NAT 130
7.10.3 Set Up a Firewall Rule 131
7.11 How to Use Multiple Static Public WAN IP Addresses for LAN to WAN Traffic 132
7.11.1 Create the Public IP Address Range Object 132
7.11.2 Configure the Policy Route 132

Chapter 8
PBX Tutorials 135

8.1 Making Internal Calls 136
8.1.1 Configure SIP Extensions 136
8.1.2 Connect IP Phones 140
8.1.3 Register IP Phones 140
8.2 Auto Provisioning 141
8.2.1 Configuring the snom VoIP Phones for Auto Provisioning 142
8.3 Making PSTN Calls 143
8.3.1 The PSTN Connection 143
8.3.2 Creating a Dialing Rule for PSTN 144
8.3.3 Assigning an LCR to an Authority Group 146
8.4 Making ITSP Calls 147
8.4.1 The ITSP Connection 148
8.4.2 Creating a Dialing Rule for ITSP 151
8.4.3 Assigning an LCR to an Authority Group 152
8.5 Making ISDN Calls 154
8.5.1 The ISDN Connection 155
8.5.2 Creating a Dialing Rule for ISDN 156
8.5.3 Assigning an LCR to an Authority Group 158
8.6 ISDN Network Configuration Examples 159
8.6.1 Example 1: Small/Medium Business 160
8.6.2 Example 2: Company with Existing PBX 161
8.6.3 Example 3: Company with Existing PBX and Expanding Employees 162

8.7 Using Call Features 163
    8.7.1 Customizing Feature Codes 163
    8.7.2 Using the Voicemail Feature 163
8.8 Using the Extension Portal 164
    8.8.1 Your Information 164
    8.8.2 Accessing the Extension Portal 164
    8.8.3 Using the Web Phone (IP Phone Users Only) 165
    8.8.4 Changing Your Security Information 166
    8.8.5 Personalizing Your Settings 167
    8.8.6 Setting Up Voicemail 170
8.9 Capturing Packets Using the Web Configurator 171
8.10 Creating an Automated Menu System 173
    8.10.1 Menu Design and Call Routing 173
    8.10.2 Create an Agent Identity 174
    8.10.3 Create a Skill 175
    8.10.4 Create an Auto-Attendant 178

Part II: Technical Reference.. 183

Chapter 9
Dashboard..185

9.1 Overview 185
    9.1.1 What You Can Do in this Chapter 185
9.2 The Dashboard Screen 185
    9.2.1 The CPU Usage Screen 190
    9.2.2 The Memory Usage Screen 190
    9.2.3 The Active Sessions Screen 191
    9.2.4 The VPN Status Screen 192
    9.2.5 The DHCP Table Screen 192
    9.2.6 The Number of Login Users Screen 193

Chapter 10
Monitor..195

10.1 Overview 195
    10.1.1 What You Can Do in this Chapter 195
10.2 The Port Statistics Screen 196
    10.2.1 The Port Statistics Graph Screen 197
10.3 Interface Status Screen 198
10.4 The Traffic Statistics Screen 200
10.5 The Session Monitor Screen 203
10.6 The DDNS Status Screen 205

10.7 IP/MAC Binding Monitor 205
10.8 The Login Users Screen 206
10.9 Cellular Status Screen 207
    10.9.1 More Information 209
10.10 USB Storage Screen 210
10.11 The IPSec Monitor Screen 211
    10.11.1 Regular Expressions in Searching IPSec SAs 212
10.12 SIP Peer Screen 213
10.13 FXS Peer Screen 214
10.14 SIP Trunk Screen 215
10.15 CTI Peer Screen 216
10.16 FXO Trunk Screen 217
10.17 BRI Trunk Screen 218
10.18 ACD Queue Screen 219
10.19 Log Screen 220
10.20 Querying Call Recordings 222
    10.20.1 Call Recordings File List 223
10.21 CDR Backup Screen 223
10.22 CDR Query Screen 225
10.23 CDR Query Result Screen 227

Chapter 11
Registration....................229

11.1 Overview 229
    11.1.1 What You Can Do in this Chapter 229
    11.1.2 What you Need to Know 229
11.2 The Registration Screen 230
11.3 The Service Screen 231

Chapter 12
Interfaces....................233

12.1 Interface Overview 233
    12.1.1 What You Can Do in this Chapter 233
    12.1.2 What You Need to Know 233
12.2 Port Role 236
12.3 Ethernet Summary Screen 237
    12.3.1 Ethernet Edit 238
    12.3.2 Object References 246
12.4 PPP Interfaces 246
    12.4.1 PPP Interface Summary 247
    12.4.2 PPP Interface Add or Edit 248
12.5 Cellular Configuration Screen (3G) 251
    12.5.1 Cellular Add/Edit Screen 253

12.6 VLAN Interfaces 259
12.6.1 VLAN Summary Screen 261
12.6.2 VLAN Add/Edit 262
12.7 Bridge Interfaces 267
12.7.1 Bridge Summary 269
12.7.2 Bridge Add/Edit 270
12.7.3 Virtual Interfaces Add/Edit 275
12.8 Interface Technical Reference 276

Chapter 13
Trunks 281

13.1 Overview 281
13.1.1 What You Can Do in this Chapter 281
13.1.2 What You Need to Know 281
13.2 The Trunk Summary Screen 285
13.3 Configuring a Trunk 287
13.4 Trunk Technical Reference 288

Chapter 14
Policy and Static Routes 289

14.1 Policy and Static Routes Overview 289
14.1.1 What You Can Do in this Chapter 289
14.1.2 What You Need to Know 290
14.2 Policy Route Screen 291
14.2.1 Policy Route Edit Screen 294
14.3 IP Static Route Screen 297
14.3.1 Static Route Add/Edit Screen 298
14.4 Policy Routing Technical Reference 299

Chapter 15
Routing Protocols 302

15.1 Routing Protocols Overview 302
15.1.1 What You Can Do in this Chapter 302
15.1.2 What You Need to Know 302
15.2 The RIP Screen 302
15.3 The OSPF Screen 304
15.3.1 Configuring the OSPF Screen 307
15.3.2 OSPF Area Add/Edit Screen 309
15.3.3 Virtual Link Add/Edit Screen 311
15.4 Routing Protocol Technical Reference 311

Chapter 16
Zones 313

16.1 Zones Overview 313
16.1.1 What You Can Do in this Chapter 313
16.1.2 What You Need to Know 313
16.2 The Zone Screen 314
16.3 Zone Edit 315

Chapter 17
DDNS.....317

17.1 DDNS Overview 317
17.1.1 What You Can Do in this Chapter 317
17.1.2 What You Need to Know 317
17.2 The DDNS Screen 318
17.2.1 The Dynamic DNS Add/Edit Screen 319

Chapter 18
NAT.....323

18.1 NAT Overview 323
18.1.1 What You Can Do in this Chapter 323
18.1.2 What You Need to Know 323
18.2 The NAT Screen 324
18.2.1 The NAT Add/Edit Screen 325
18.3 NAT Technical Reference 328

Chapter 19
HTTP Redirect.....331

19.1 Overview 331
19.1.1 What You Can Do in this Chapter 331
19.1.2 What You Need to Know 331
19.2 The HTTP Redirect Screen 332
19.2.1 The HTTP Redirect Edit Screen 333

Chapter 20
ALG 335

20.1 ALG Overview 335
20.1.1 What You Can Do in this Chapter 335
20.1.2 What You Need to Know 335
20.1.3 Before You Begin 337
20.2 The ALG Screen 338
20.3 ALG Technical Reference 339

Chapter 21
IP/MAC Binding.....341

21.1 IP/MAC Binding Overview 341

21.1.1 What You Can Do in this Chapter 341
21.1.2 What You Need to Know 341
21.2 IP/MAC Binding Summary 342
21.2.1 IP/MAC Binding Edit 343
21.2.2 Static DHCP Edit 344
21.3 IP/MAC Binding Exempt List 345

Chapter 22
Authentication Policy 347

22.1 Overview 347
22.1.1 What You Can Do in this Chapter 347
22.1.2 What You Need to Know 347
22.2 Authentication Policy Screen 347
22.2.1 Creating/Editing an Authentication Policy 350

Chapter 23
Firewall 353

23.1 Overview 353
23.1.1 What You Can Do in this Chapter 353
23.1.2 What You Need to Know 354
23.1.3 Firewall Rule Example Applications 356
23.1.4 Firewall Rule Configuration Example 358
23.2 The Firewall Screen 360
23.2.1 Configuring the Firewall Screen 360
23.2.2 The Firewall Add/Edit Screen 363
23.3 The Session Limit Screen 364
23.3.1 The Session Limit Add/Edit Screen 365

Chapter 24
IPSec VPN....................367

24.1 IPSec VPN Overview 367
24.1.1 What You Can Do in this Chapter 367
24.1.2 What You Need to Know 368
24.1.3 Before You Begin 370
24.2 The VPN Connection Screen 370
24.2.1 The VPN Connection Add/Edit (IKE) Screen 371
24.2.2 The VPN Connection Add/Edit Manual Key Screen 377
24.3 The VPN Gateway Screen 379
24.3.1 The VPN Gateway Add/Edit Screen 381
24.4 IPSec VPN Background Information 386

Chapter 25
Bandwidth Management....................397

25.1 Overview 397
25.1.1 What You Can Do in this Chapter 397
25.1.2 What You Need to Know 397
25.1.3 Bandwidth Management Examples 401
25.2 The Bandwidth Management Screen 404
25.2.1 The Bandwidth Management Add/Edit Screen 406

Chapter 26
ADP 411

26.1 Overview 411
26.1.1 ADP 411
26.1.2 What You Can Do in this Chapter 411
26.1.3 What You Need To Know 411
26.1.4 Before You Begin 412
26.2 The ADP General Screen 412
26.3 The Profile Summary Screen 413
26.3.1 Base Profiles 414
26.3.2 Configuring The ADP Profile Summary Screen 414
26.3.3 Creating New ADP Profiles 415
26.3.4 Traffic Anomaly Profiles 415
26.3.5 Protocol Anomaly Profiles 418
26.3.6 Protocol Anomaly Configuration 418
26.4 ADP Technical Reference 421

Chapter 27
Global PBX Settings 429

27.1 Overview 429
27.1.1 What You Can Do in this Chapter 429
27.1.2 What You Need to Know 430
27.2 The SIP Server Screen 431
27.3 The Feature Code Screen 433
27.4 The E-Mail Screen 435
27.5 The Fake IP Screen 435
27.6 The Peer to Peer Screen 436
27.6.1 How the Peer-to-Peer SIP Connection Works 437
27.6.2 Add Peer-to-Peer Local Net 438
27.6.3 How Local Net and Peer-to-Peer Work Together 439
27.7 The QoS Screen 440
27.8 The TAPI Screen 442
27.8.1 Setting Up the TAPI Driver and Utility on Your Computer 443
27.9 Network Technical Reference 447

Chapter 28
Voice Interfaces 448

28.1 Overview 448
28.1.1 What You Can Do in this Chapter 448
28.1.2 What You Need to Know 448
28.2 The FXS Screen 449
28.3 The FXO Screen 450
28.4 The BRI Screen 451

Chapter 29
Extension Management..453

29.1 Overview 453
29.1.1 What You Can Do in this Chapter 453
29.1.2 What You Need to Know 453
29.1.3 Before You Begin 457
29.2 The Authority Group Screen 458
29.2.1 The Add Authority Group Screen 458
29.2.2 The Authority Group Edit Screen 459
29.3 Extension Features 461
29.3.1 Extension Add/Edit the Basic Screen 462
29.3.2 The Extension Call Forward Screen 463
29.3.3 The Extension Voice Mail Settings Screen 467
29.3.4 The Extension Advanced Screen 468
29.3.5 The Batch Add SIP Screen 469
29.4 The Group Access Code Screen 471
29.5 The Click To Talk Group Screen 472
29.5.1 Add or Edit a Click To Talk Group 472
29.6 Authority Group Technical Reference 475

Chapter 30
Outbound Trunk Group 477

30.1 Overview 477
30.1.1 What You Can Do in this Chapter 477
30.1.2 What You Need to Know 478
30.1.3 Before You Begin 481
30.2 Outbound Trunk Group Screen 481
30.2.1 SIP Trunk Add/Edit 483
30.2.2 SIP Auto Attendant and DDI Setup 486
30.2.3 Add DDI/DID Number 488
30.2.4 Trusted Peer Trunk Add/Edit 490
30.2.5 Trusted Peer Auto Attendant and DDI Setup 493
30.2.6 Add/Edit FXO Trunk 495
30.2.7 FXO or BRI Auto Attendant 496
30.2.8 Add/Edit BRI Trunk 497
30.2.9 Add BRI Trunk DDI/DID Mapping 502

30.2.10 Auto-Attendant for Incoming BRI Calls 502

Chapter 31
Auto-attendant 503

31.1 Overview 503
31.1.1 What You Can Do in this Chapter 503
31.1.2 What You Need to Know 503
31.2 The Default Auto-Attendant Screen 505
31.3 The Customized Auto-Attendant Screen 507
31.3.1 The Add/Edit Auto-Attendant Screen 508
31.3.2 Auto Attendant Settings: Office Hours 509
31.3.3 The Add/Edit Auto-Attendant Option Screen 511
31.3.4 The Auto-Attendant Sub Menu Screen 512
31.3.5 Auto Attendant Settings: Night Service 513
31.3.6 Greeting 515
31.4 Technical Reference 516

Chapter 32
LCR 519

32.1 Overview 519
32.1.1 What You Can Do in this Chapter 520
32.1.2 What You Need to Know 520
32.1.3 Before You Begin 520
32.2 LCR 521
32.2.1 LCR Configuration 521
32.2.2 Add/Edit LCR Dial Condition 523

Chapter 33
Group Management 526

33.1 Overview 526
33.1.1 What You Can Do in this Chapter 527
33.1.2 What You Need to Know 527
33.1.3 Before You Begin 530
33.2 Group Management Screen 530
33.2.1 Edit Group Management Associations 531

Chapter 34
Call Services 532

34.1 Overview 532
34.1.1 What You Can Do in this Chapter 532
34.1.2 What You Need to Know 532
34.1.3 Before You Begin 533
34.2 The Auto Callback Screen 533

34.3 The Call Park Screen 534
34.3.1 Configuring the Call Park Screen 535
34.4 The Call Waiting Screen 536
34.4.1 Configuring the Call Waiting Screen 537
34.5 The Emergency Call Screen 538
34.5.1 Configuring the Emergency Call Screen 538
34.6 The Music on Hold Screen 539
34.6.1 Add or Edit Custom Music On Hold 541
34.7 The Call Transfer Screen 541
34.7.1 Configuring the Call Transfer Screen 542
34.8 The Call Block Screen 542

Chapter 35
Call Recording 544

35.1 Overview 544
35.1.1 What You Can Do in this Chapter 544
35.1.2 What You Need to Know 544
35.2 Configuring the Call Recording Screen 545

Chapter 36
Meet-me Conference 547

36.0.1 Configuring the Meet-me Conference Screen 547
36.0.2 The Meet-me Conference Calling Edit and Add Screen 547

Chapter 37
Paging Group 549

37.1 Overview 549
37.2 The Paging Group Screen 549
37.2.1 The Add/Edit Paging Group Screen 550

Chapter 38
ACD 553

38.1 Overview 553
38.1.1 What You Can Do in this Chapter 553
38.1.2 What You Need to Know 554
38.2 The ACD Global Screen 556
38.3 The Agent Screen 556
38.3.1 The Agent Settings Screen 557
38.4 The Skill Screen 558
38.4.1 The Add/Edit Skill Screen 559
38.5 The Hunt Group Screen 562
38.5.1 The Add/Edit Hunt Group Screen 563
38.6 The Skill Menu Screen 564

38.6.1 The Skill Menu Settings Screen 565
38.6.2 Add/Edit Skill Menu Action Screen 566

Chapter 39
Sound Files 568

39.1 Overview 568
39.1.1 What You Can Do in this Chapter 568
39.1.2 What You Need to Know 568
39.2 The System Sound Screen 568
39.2.1 The Add/Edit Sound File Screen 569
39.3 The Specific Sound File Screen 570
39.3.1 The Add/Edit Sound File Screen 571
39.4 The Record Peer Screen 571

Chapter 40
Auto Provision 573

40.1 Overview 573
40.1.1 What You Can Do in this Chapter 573
40.1.2 What You Need to Know 573
40.1.3 Before You Begin 574
40.2 Auto Provision Setup 575
40.2.1 snom Batch Configuration XML File 576
40.2.2 Auto Provision Edit 577
40.3 Auto Provision Advanced Screen 578

Chapter 41
Voice Mail 581

41.1 Overview 581
41.1.1 What You Can Do in this Chapter 581
41.1.2 What You Need to Know 581
41.2 The Voice Mail Screen 582
41.3 Accessing Voice Mail 583

Chapter 42
Phonebook 587

42.1 Overview 587
42.1.1 What You Can Do in this Chapter 587
42.1.2 What You Need to Know 587
42.1.3 Before You Begin 588
42.2 The Phonebook General Screen 588
42.3 The LDAP Phonebook Summary Screen 589
42.4 The LDAP Phonebook Settings Screen 589
42.5 The Local Phonebook Screen 591

42.5.1 Local Phonebook Add/Edit Screen 592

Chapter 43
Office Hours 595

43.1 Overview 595
43.1.1 What You Can Do in this Chapter 595
43.1.2 What You Need To Know 595
43.1.3 Before You Begin 595
43.2 Office Hour Screen 595

Chapter 44
User/Group 599

44.1 Overview 599
44.1.1 What You Can Do in this Chapter 599
44.1.2 What You Need To Know 599
44.2 User Summary Screen 601
44.2.1 User Add/Edit Screen 602
44.3 User Group Summary Screen 604
44.3.1 Group Add/Edit Screen 605
44.4 Setting Screen 605
44.4.1 Default User Authentication Timeout Settings Edit Screens 608
44.4.2 User Aware Login Example 609
44.5 User /Group Technical Reference 610

Chapter 45
Addresses 613

45.1 Overview 613
45.1.1 What You Can Do in this Chapter 613
45.1.2 What You Need To Know 613
45.2 Address Summary Screen 613
45.2.1 Address Add/Edit Screen 614
45.3 Address Group Summary Screen 615
45.3.1 Address Group Add/Edit Screen 616

Chapter 46
Services 619

46.1 Overview 619
46.1.1 What You Can Do in this Chapter 619
46.1.2 What You Need to Know 619
46.2 The Service Summary Screen 620
46.2.1 The Service Add/Edit Screen 622
46.3 The Service Group Summary Screen 622
46.3.1 The Service Group Add/Edit Screen 624

Chapter 47
Schedules...625

47.1 Overview 625
47.1.1 What You Can Do in this Chapter 625
47.1.2 What You Need to Know 625
47.2 The Schedule Summary Screen 626
47.2.1 The One-Time Schedule Add/Edit Screen 627
47.2.2 The Recurring Schedule Add/Edit Screen 628

Chapter 48
AAA Server...631

48.1 Overview 631
48.1.1 Directory Service (AD/LDAP) 631
48.1.2 RADIUS Server 631
48.1.3 ASAS 632
48.1.4 What You Can Do in this Chapter 632
48.1.5 What You Need To Know 632
48.2 Active Directory or LDAP Server Summary 634
48.2.1 Adding an Active Directory or LDAP Server 635
48.3 RADIUS Server Summary 636
48.3.1 Adding a RADIUS Server 637

Chapter 49
Authentication Method..639

49.1 Overview 639
49.1.1 What You Can Do in this Chapter 639
49.1.2 Before You Begin 639
49.1.3 Example: Selecting a VPN Authentication Method 639
49.2 Authentication Method Objects 640
49.2.1 Creating an Authentication Method Object 641

Chapter 50
Certificates 643

50.1 Overview 643
50.1.1 What You Can Do in this Chapter 643
50.1.2 What You Need to Know 643
50.1.3 Verifying a Certificate 645
50.2 The My Certificates Screen 646
50.2.1 The My Certificates Add Screen 648
50.2.2 The My Certificates Edit Screen 651
50.2.3 The My Certificates Import Screen 653
50.3 The Trusted Certificates Screen 654
50.3.1 The Trusted Certificates Edit Screen 656

50.3.2 The Trusted Certificates Import Screen 659
50.4 Certificates Technical Reference 659

Chapter 51
ISP Accounts

ISP Accounts 661

51.1 Overview 661
51.1.1 What You Can Do in this Chapter 661
51.2 ISP Account Summary 661
51.2.1 ISP Account Add/Edit 662

Chapter 52
System

System 665

52.1 Overview 665
52.1.1 What You Can Do in this Chapter 665
52.2 Host Name 666
52.3 USB Storage 666
52.4 Date and Time 667
52.4.1 Pre-defined NTP Time Servers List 670
52.4.2 Time Server Synchronization 670
52.5 Console Port Speed 671
52.6 DNS Overview 672
52.6.1 DNS Server Address Assignment 672
52.6.2 Configuring the DNS Screen 672
52.6.3 Address Record 674
52.6.4 PTR Record 675
52.6.5 Adding an Address/PTR Record 675
52.6.6 Domain Zone Forwarder 675
52.6.7 Adding a Domain Zone Forwarder 676
52.6.8 MX Record 676
52.6.9 Adding a MX Record 677
52.6.10 Adding a DNS Service Control Rule 677
52.7 WWW Overview 678
52.7.1 Service Access Limitations 678
52.7.2 System Timeout 678
52.7.3 HTTPS 679
52.7.4 Configuring WWW Service Control 680
52.7.5 Service Control Rules 683
52.7.6 Customizing the WWW Login Page 683
52.7.7 HTTPS Example 687
52.8 SSH 693
52.8.1 How SSH Works 694
52.8.2 SSH Implementation on the ISG50 695
52.8.3 Requirements for Using SSH 695

52.8.4 Configuring SSH 695
52.8.5 Secure Telnet Using SSH Examples 696
52.9 Telnet 698
52.9.1 Configuring Telnet 698
52.10 FTP 699
52.10.1 Configuring FTP 699
52.11 SNMP 700
52.11.1 Supported MIBs 702
52.11.2 SNMP Traps 702
52.11.3 Configuring SNMP 702
52.12 Language Screen 704

Chapter 53
Log and Report 705

53.1 Overview 705
53.1.1 What You Can Do In this Chapter 705
53.2 Email Daily Report 705
53.3 Log Setting Screens 707
53.3.1 Log Setting Summary 708
53.3.2 Edit System Log Settings 710
53.3.3 Edit Log on USB Storage Setting 713
53.3.4 Edit Remote Server Log Settings 715
53.3.5 Active Log Summary Screen 716

Chapter 54
Call Detail Record (CDR) 720

54.1 Overview 720
54.1.1 What You Can Do in this Chapter 720
54.1.2 What You Need to Know 720
54.2 The CDR Configuration Screen 721
54.2.1 Configure Your Remote Server 722

Chapter 55
File Manager 725

55.1 Overview 725
55.1.1 What You Can Do in this Chapter 725
55.1.2 What you Need to Know 725
55.2 The Configuration File Screen 727
55.3 The Firmware Package Screen 731
55.4 The Shell Script Screen 733

Chapter 56
Diagnostics 737

56.1 Overview 737
56.1.1 What You Can Do in this Chapter 737
56.2 The Diagnostic Screen 737
56.2.1 The Diagnostics Files Screen 738
56.3 The Packet Capture Screen 739
56.3.1 The Packet Capture Files Screen 741
56.3.2 Example of Viewing a Packet Capture File 742
56.4 Core Dump Screen 742
56.4.1 Core Dump Files Screen 743
56.5 The System Log Screen 744

Chapter 57
Packet Flow Explore....745

57.1 Overview 745
57.1.1 What You Can Do in this Chapter 745
57.2 The Routing Status Screen 745
57.3 The SNAT Status Screen 750

Chapter 58
Reboot 753

58.1 Overview 753
58.1.1 What You Need To Know 753
58.2 The Reboot Screen 753

Chapter 59
Shutdown....755

59.1 Overview 755
59.1.1 What You Need To Know 755
59.2 The Shutdown Screen 755

Chapter 60
Extension Portal....757

60.1 Overview 757
60.1.1 What You Can Do in this Chapter 757
60.1.2 What You Need to Know 758
60.2 Web Phone 759
60.3 Peer Info 760
60.4 Call Forwarding and Blocking 761
60.5 Voice Mail Settings 763
60.6 Call Recording 764

Chapter 61
Troubleshooting....765

61.1 Resetting the ISG50 774
61.2 Getting More Troubleshooting Help 774

Appendix A Log Descriptions...775

Appendix B Common Services...827

Appendix C Importing Certificates 831

Appendix D Legal Information 855

Index 857

PART I

User's Guide

1

Introducing the ISG50

This chapter gives an overview of the ISG50. It explains the front panel ports, LEDs, introduces the management methods, and lists different ways to start or stop the ISG50.

1.1 Overview

The ISG50 combines an IP PBX with powerful routing and security features. Its flexible configuration helps network administrators set up the network and enforce security policies efficiently, making it an ideal solution for reliable, secure voice and data service.

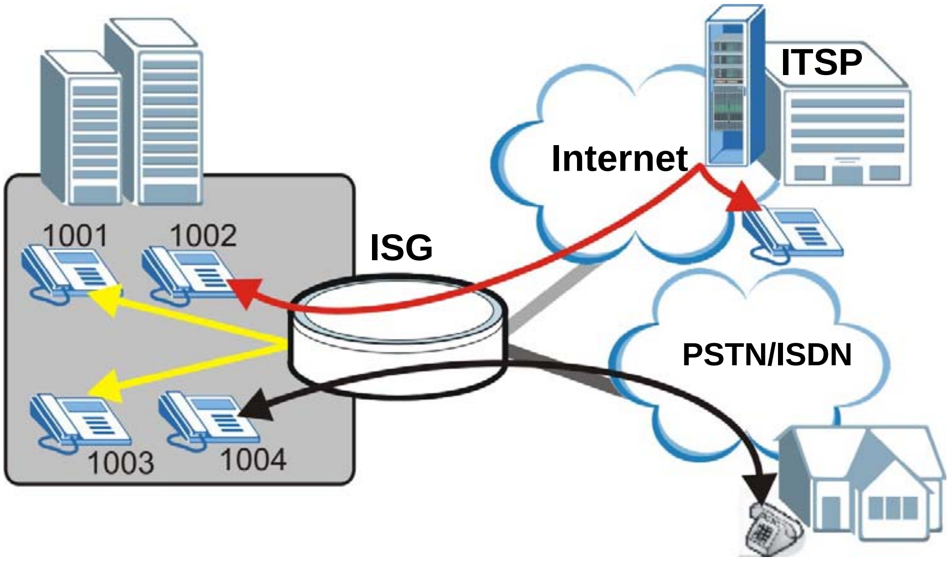
1.1.1 PBX

An IP PBX is a telephone exchange device located at a company site which allows an organization to set up and control calls. IP stands for Internet Protocol, and PBX stands for Private Branch Exchange. A regular company telephone switchboard is an example of a PBX. The company's telephones are connected to the IP PBX. The IP PBX is then connected to the outside world via connections to a combination of the following networks:

- A traditional Public Switched Telephone Network (PSTN): ISG50-PSTN
- An Internet connection to an Internet Telephony Service Provider (ITSP): all ISG50 models
- An Integrated Services Digital Network/Basic Rate Interface Network (ISDN BRI): ISG50-ISDN

Each telephone connected to an IP PBX has an extension assigned to it. An extension is a unique telephone number within an organization typically consisting of only a few digits. People inside the company can call each other by dialing extensions. Calls to the outside world go through the IP PBX to the PSTN, ITSP, or ISDN.

Figure 1 IP PBX Example



The ISG50 can function as a stand alone telephone switchboard for a small organization. It can also supplement a legacy PBX within an organization by providing VoIP telephony features. See Chapter 2 on page 37 for a more detailed overview of the ISG50's features.

1.1.2 Security and Routing

The ISG50's security features include VPN, firewall, ADP (Anomaly Detection and Protection), and certificates. It also provides bandwidth management, Instant Messaging (IM) and Peer to Peer (P2P) control, NAT, port forwarding, policy routing, DHCP server and other powerful features. Flexible configuration helps you set up the network and enforce security policies efficiently. See Chapter 2 on page 37 for a more detailed overview of the ISG50's features.

The ISG50 provides excellent throughput with the reliability of dual WAN Gigabit Ethernet ports and load balancing. You can also use a 3G cellular USB (not included) for a third WAN connection.

The ISG50 lets you set up multiple networks for your company. The De-Militarized Zone (DMZ) increases LAN security by providing separate ports for connecting publicly accessible servers. The ISG50 also provides two separate LAN networks. You can set ports to be part of the LAN1, or DMZ. Alternatively, you can deploy the ISG50 as a transparent firewall in an existing network with minimal configuration.

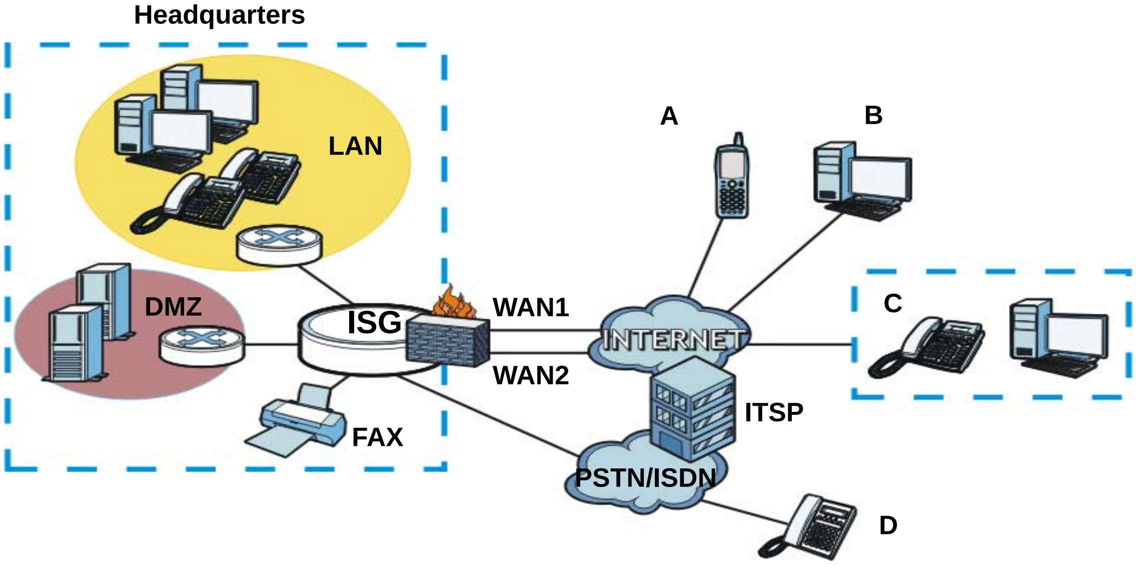
1.1.3 Application Scenarios

Here are some common application scenarios for the ISG50.

1.1.3.1 All-in-one

Use the ISG50 to provide VoIP and security services.

Figure 2 All-in-one Application Scenario



VoIP Services:

- VoIP phones and smartphones can make internal calls and external calls.
- Least Cost Routing (LCR) dialing rules put calls through the appropriate outbound line. Long distance calls (to C in the figure) use VoIP and local calls (to **D**) use PSTN or ISDN.
- Auto attendant menu systems act as automatic switchboard operators to help route incoming calls to the proper extension.
- Customers (like **B**) use Web services such as Click To Talk, Skype, or Google Voice to call in.
- Voice mail stores voice messages for users and can also forward them by email.
- Conference room extensions allow callers from within and outside your organization to join conference calls by dialing a conference room extension.
- Use call recording to record all calls for specific extensions or trunks or let users record calls.
- VLAN and QoS enhance voice quality.
- Fax over IP.
- PSTN or ISDN outbound voice trunks and fax service.

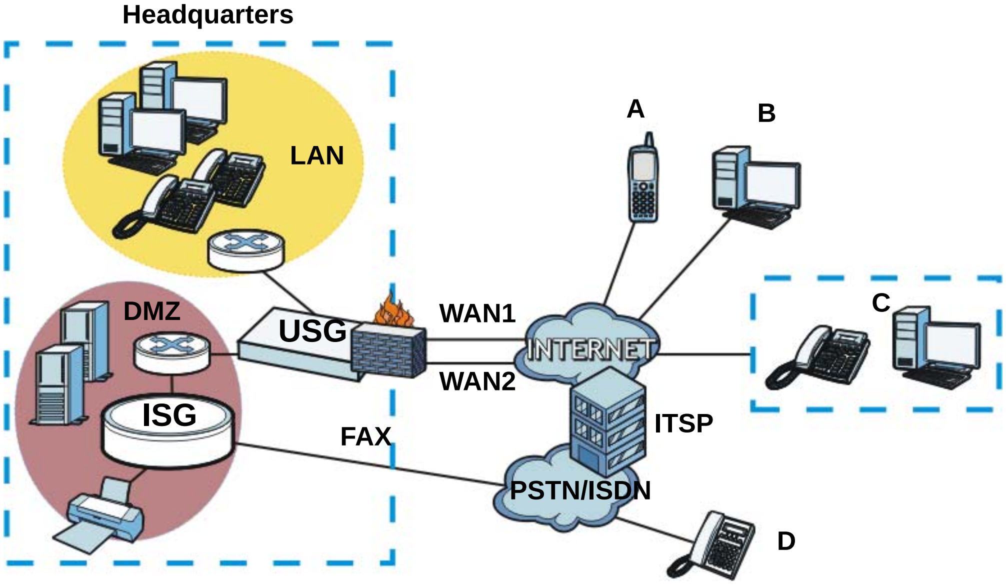
Security Services:

- Firewall protected Internet access and DMZ network for publicly accessible servers.
- IPSec VPN-secured VoIP services and internal server access for teleworkers (**A** and **C** in the diagram).
- Multiple WAN gives fail-over protection for VPN connections and VoIP.

1.1.3.2 DMZ Installation

Use the ISG50 with a USG, ZyXEL's Unified Threat Management (UTM) firewall to add more security services like IDP and anti-virus. If you connect the ISG50 to a USG model's DMZ, the ISG50 provides the VoIP services listed in the previous scenario, and the USG provides the security services. Here is an example.

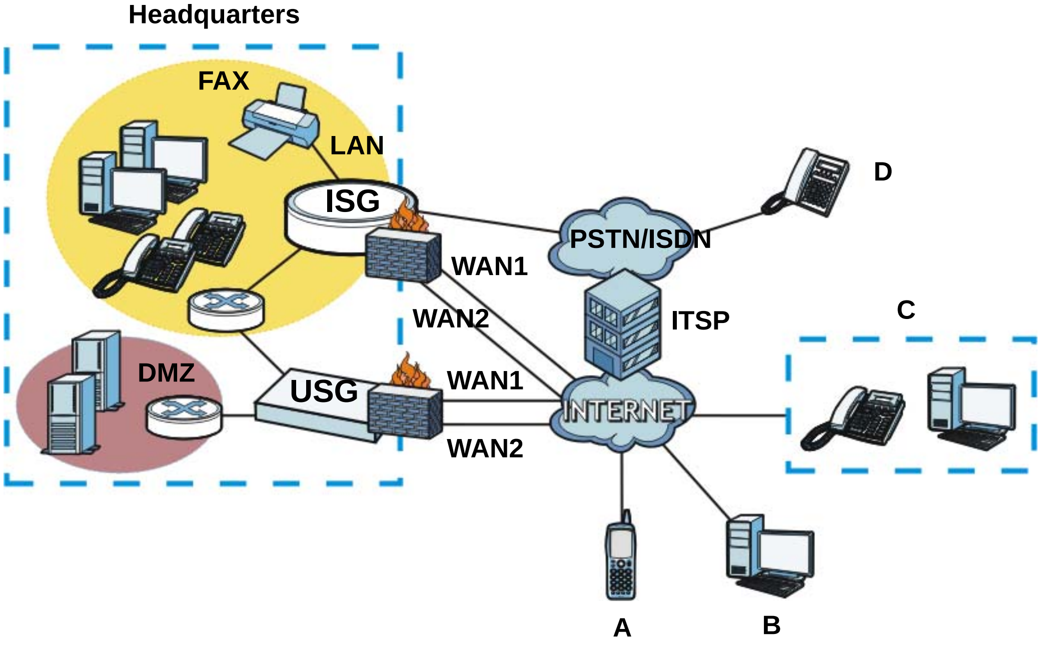
Figure 3 DMZ Installation


Headquarters
LAN
DMZ
USG
ISG
A
B
C
WAN1
WAN2
INTERNET
ITSP
FAX
PSTN/ISDN
D

1.1.3.3 Parallel to a USG

Connect the ISG50 to the Internet and a USG model's LAN to give the VoIP a physically separate Internet connection to keep bursts of data traffic from impacting voice quality. The ISG50 provides the VoIP services listed in the previous scenario along with firewall protection and VPN and WAN fail-over for the VoIP services. The USG provides additional WAN fail-over protection for the VoIP services. Here is an example of using the ISG50 along with a USG.

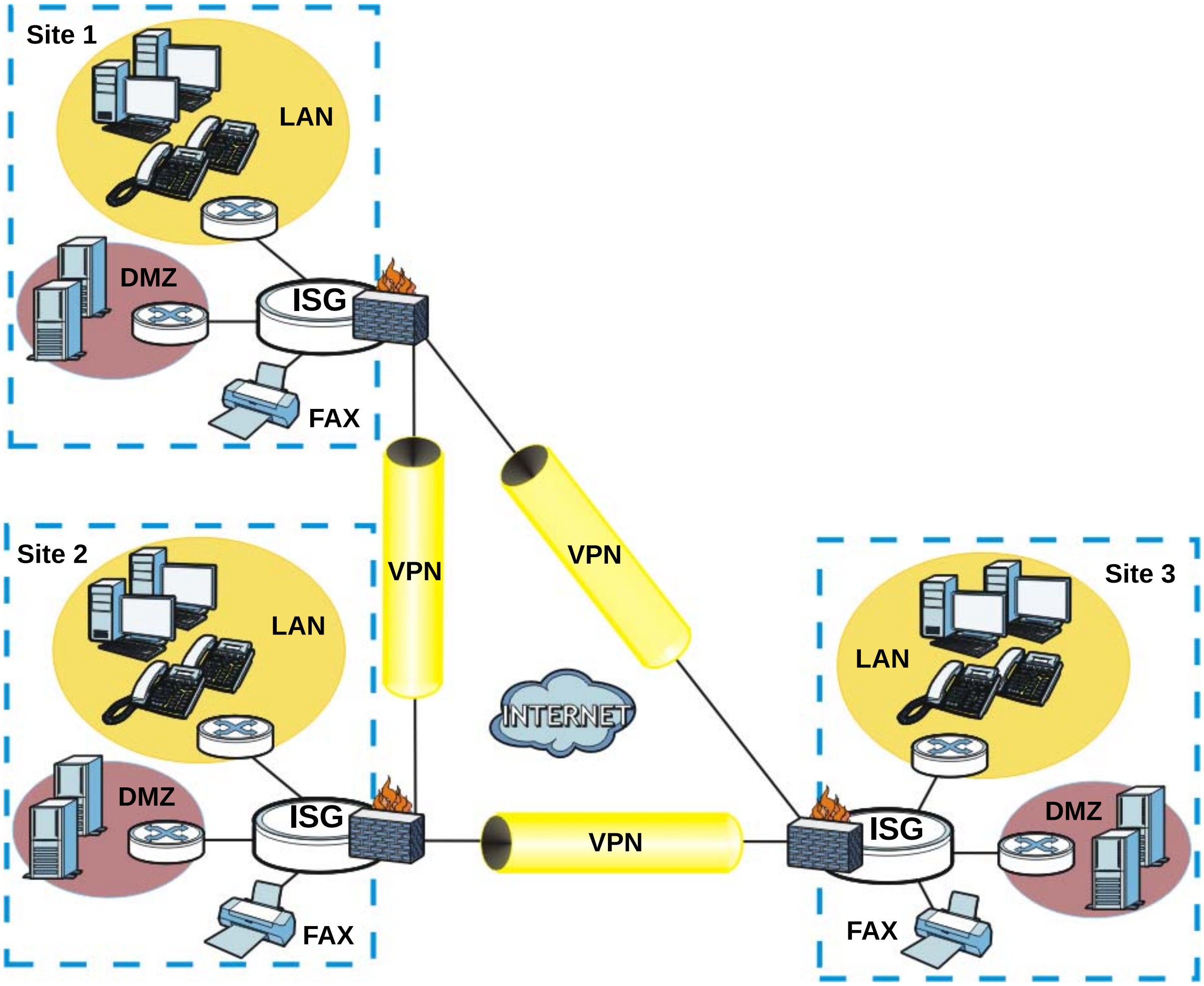
Figure 4 Installation Parallel to a USG


Headquarters
FAX
LAN
ISG
WAN1
WAN2
DMZ
USG
WAN1
WAN2
PSTN/ISDN
D
ITSP
C
INTERNET
A
B

1.1.3.4 N-site

In addition to one of the application scenarios already described, you can also use site-to-site VPNs to connect ISG50s at multiple locations. This allows peer to peer VoIP calling and faxes over IP without using an ITSP and remote dial-out to make local calls in different areas. For example, with ISG50s at offices in the US and Germany, if someone in the US office needs to call someone in Germany, you can route the call through the Internet and out through the German office so it gets billed as a local German call.

Figure 5 N-Site Application



1.2 Rack-mounted Installation

The ISG50 can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your ISG50 on a standard EIA rack using a rack-mounting kit. Make sure the rack will safely support the combined weight of all the equipment it contains and that the position of the ISG50 does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

Note: Leave 10 cm of clearance at the sides and 20 cm in the rear.

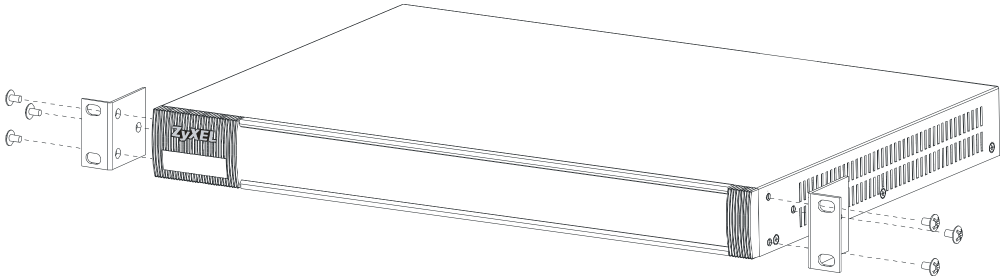
Use a #2 Phillips screwdriver to install the screws.

Note: Failure to use the proper screws may damage the unit.

1.2.1 Rack-Mounted Installation Procedure

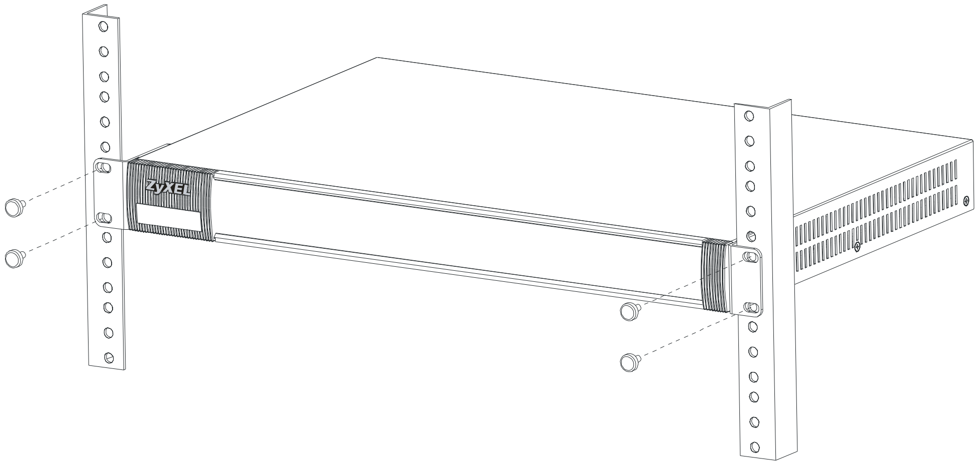
1. Align one bracket with the holes on one side of the ISG50 and secure it with the included bracket screws (smaller than the rack-mounting screws).
2. Attach the other bracket in a similar fashion.

Figure 6 Attaching Mounting Brackets and Screws



3. After attaching both mounting brackets, position the ISG50 in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the ISG50 to the rack with the rack-mounting screws.

Figure 7 Rack Mounting



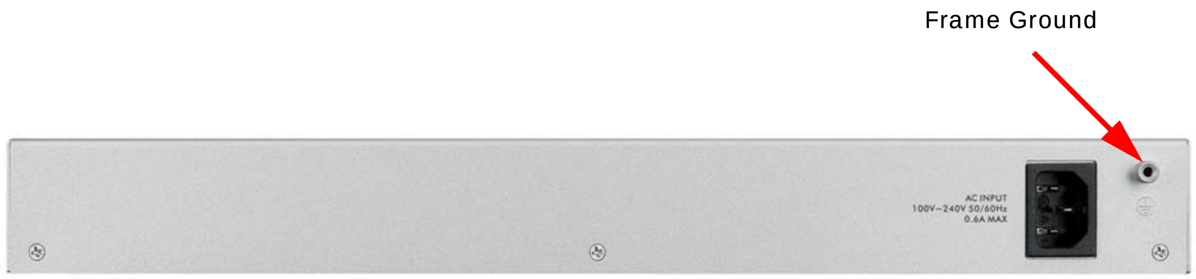
1.3 Connecting the Frame Ground

Connect the frame ground on the rear panel to a building’s protective earthing terminals.

Use a 18 AWG or larger green-and-yellow frame ground wire.

Connect the frame ground before you connect any other cables or wiring.

Figure 8 Frame Ground


Frame Ground
AC INPUT
100V~240V 50/60Hz
0.6A MAX

1.4 Front Panel

This section introduces the ISG50's front panel.

Figure 9 ISG50-PSTN Front Panel

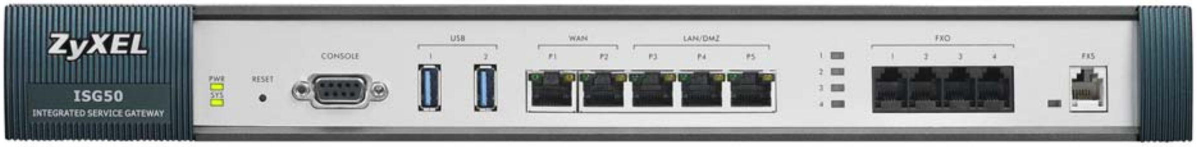
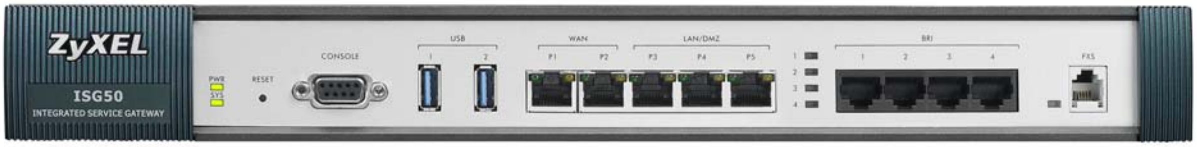

ZyXEL
ISG50
INTEGRATED SERVICE GATEWAY
PWR
SYS
RESET
CONSOLE
USB
1
2
WAN
P1
P2
LAN/DMZ
P3
P4
P5
FXO
1
2
3
4
FXS

Figure 10 ISG50-ISDN Front Panel


ZyXEL
ISG50
INTEGRATED SERVICE GATEWAY
PWR
SYS
RESET
CONSOLE
USB
1
2
WAN
P1
P2
LAN/DMZ
P3
P4
P5
BRI
1
2
3
4
FXS

1.4.1 Front Panel LEDs

The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ISG50 is turned off.
	Green	On	The ISG50 is turned on.
	Red	On	There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device (see Section 1.7 on page 35). If the LED turns red again, then please contact your vendor.
SYS	Green	Off	The ISG50 is not ready or has failed.
		On	The ISG50 is ready and running.
		Blinking	The ISG50 is booting.
	Red	On	The ISG50 had an error or has failed.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
WAN P1/P2		Off	There is no traffic on this port.
	Green	On	The Ethernet port has a successful 10/100M connection but is not sending or sending packets.
		Blinking	The ISG50 is sending or receiving packets on this port through a 10/100M connection.
	Yellow	On	The Ethernet port has a successful 1000M connection but is not sending or sending packets.
		Blinking	The ISG50 is sending or receiving packets on this port through a 10/100M connection.
LAN/DMZ P3~P5		Off	There is no traffic on this port.
	Green	On	The Ethernet port has a successful 10/100M connection but is not sending or sending packets.
		Blinking	The ISG50 is sending or receiving packets on this port through a 10/100M connection.
	Yellow	On	The Ethernet port has a successful 1000M connection but is not sending or sending packets.
		Blinking	The ISG50 is sending or receiving packets on this port through a 1000M connection.
FXO	Green	Off	The port is not connected, on-hook, or malfunctioning.
		Blinking	The port is ringing.
		On	The port is off hook.
BRI	Green	Off	The port is malfunctioning or ISDN layer 1 is deactivated.
		Blinking	The port has at least one connection active.
		On	The port has ISDN layer 1 activated.
FXS	Green	Off	The port is not connected, on-hook, or malfunctioning.
		Blinking	The port is ringing.
		On	The port is off hook.

1.5 3G PCMCIA Card Installation

Only insert a compatible 3G card. Slide the connector end of the card into the slot.

Do not force, bend or twist the card.

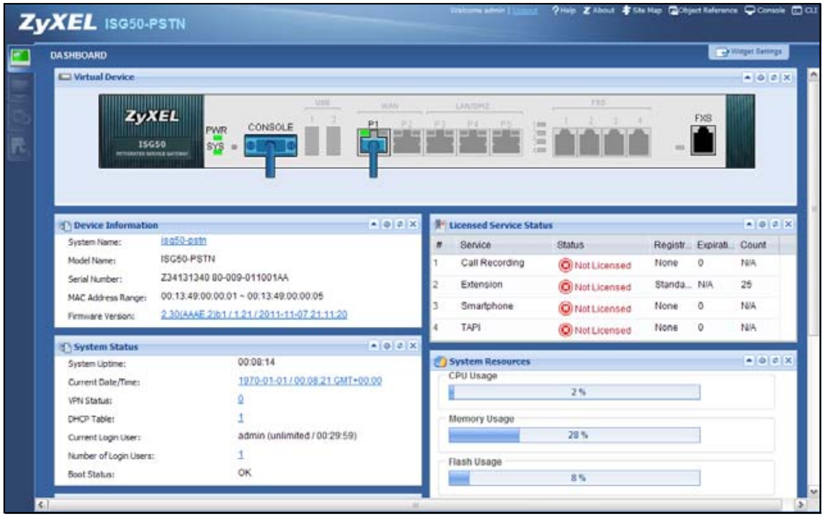
1.6 Management Overview

You can use the following ways to manage the ISG50.

Web Configurator

The Web Configurator allows easy ISG50 setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

Figure 11 Managing the ISG50: Web Configurator



System Name: isg50-pstn
Model Name: ISG50-PSTN
Serial Number: Z34131340 00-009-011001AA
MAC Address Range: 00:13:49:00:00:01 ~ 00:13:49:00:00:05
Firmware Version: 2.30(AAAE.2)b1 / 1.21 / 2011-11-07 21:11:20

System Uptime: 00:08:14
Current Date/Time: 1970-01-01 / 00:08:21 GMT+00:00
VPN Status: 0
DHCP Table: 1
Current Login User: admin (unlimited / 00:29:59)
Number of Login Users: 1
Boot Status: OK

#	Service	Status	Registr...	Expirati...	Count
1	Call Recording	Not Licensed	None	0	N/A
2	Extension	Not Licensed	Standa...	N/A	25
3	Smartphone	Not Licensed	None	0	N/A
4	TAPI	Not Licensed	None	0	N/A

CPU Usage: 2 %
Memory Usage: 28 %
Flash Usage: 8 %

Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the ISG50. You can access it using remote management (for example, SSH or Telnet) or via the console port. See the Command Reference Guide for more information about the CLI.

Console Port

You can use the console port to manage the ISG50 using CLI commands. See the Command Reference Guide for more information about the CLI.

The default settings for the console port are as follows.

Table 2 Console Port Default Settings

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

1.7 Starting and Stopping the ISG50

Here are some of the ways to start and stop the ISG50.

Always use Maintenance > Shutdown > Shutdown or the `shutdown` command before you turn off the ISG50 or remove the power. Not doing so can cause the firmware to become corrupt.

Table 3 Starting and Stopping the ISG50

METHOD	DESCRIPTION
Turning on the power	A cold start occurs when you turn on the power to the ISG50. The ISG50 powers up, checks the hardware, and starts the system processes.
Rebooting the ISG50	A warm start (without powering down and powering up again) occurs when you use the **Reboot** button in the **Reboot** screen or when you use the `reboot` command. The ISG50 writes all cached data to the local storage, stops the system processes, and then does a warm start.
Using the RESET button	If you press the **RESET** button, the ISG50 sets the configuration to its default values and then reboots.
Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command	Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command writes all cached data to the local storage and stops the system processes. Wait for the device to shut down and then manually turn off or remove the power. It does not turn off the power.
Disconnecting the power	Power off occurs when you turn off the power to the ISG50. The ISG50 simply turns off. It does not stop the system processes or write cached data to local storage.

The ISG50 does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

2

Features and Applications

This chapter introduces the main features and applications of the ISG50.

2.1 Features

Voice over Internet Protocol (VoIP) Implementation

The ISG50 uses SIP (Session Initiation Protocol) to communicate with other SIP devices. SIP is an internationally-recognized standard for implementing Voice over Internet Protocol (VoIP).

The following figure shows SIP devices communicating with the ISG50.

A: IP Phones - Telephones that convert voice into IP packets and vice versa (for example ZyXEL's V-500).

B: Softphones - Software-based phones installed on PCs.

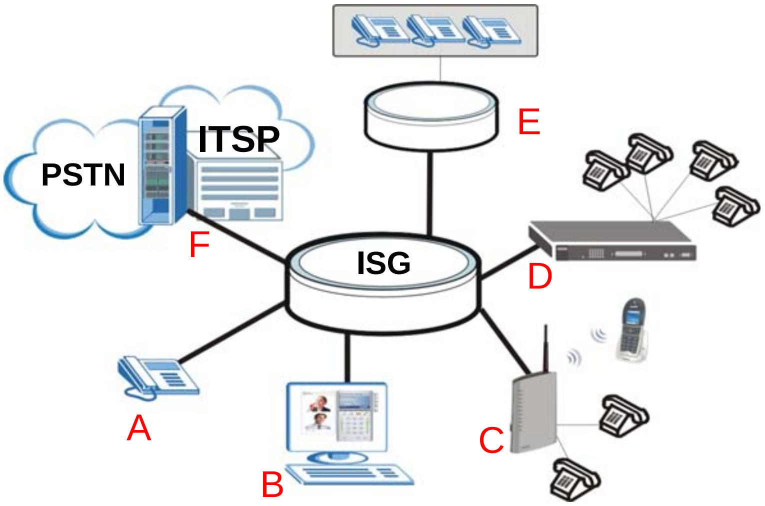
C: VoIP Gateways - Devices (for example ZyXEL's P-2302HWUDL) with built in SIP processing which allow traditional analog phones or cordless phones to use them as a link to the IP PBX.

D: ATAs - Analog Telephone Adapters (for example ZyXEL's P-2024) aggregate a large number of analog phones and convert their signal into IP packets.

E: Peer IP PBXs - Other SIP based IP PBXs with which you communicate over an IP network. This allows you to call the telephones connected to the peer IP PBX without going through a telephone service provider.

F: SIP Servers - Servers (**D**) located at your Internet Telephony Service Provider (ITSP) which process outgoing calls from the ISG50 and direct them to IP phones on the Internet or traditional phones on the PSTN.

Figure 12 SIP Devices and the ISG50



PBX Telephony Features

The ISG50 allows you to set up and manage features on an internal telephone network without relying on your telephone service provider. The following are just a few examples:

- Conference calls
- Voicemail
- Call Forwarding

The ISG50 integrates with your IP network. For example you can:

- Import an LDAP-based (Lightweight Directory Access Protocol) contact list to serve as the phonebook for the IP phones on your network.
- Set up the ISG50 to send users email notifications or complete voice messages as attachments when they receive voicemail.

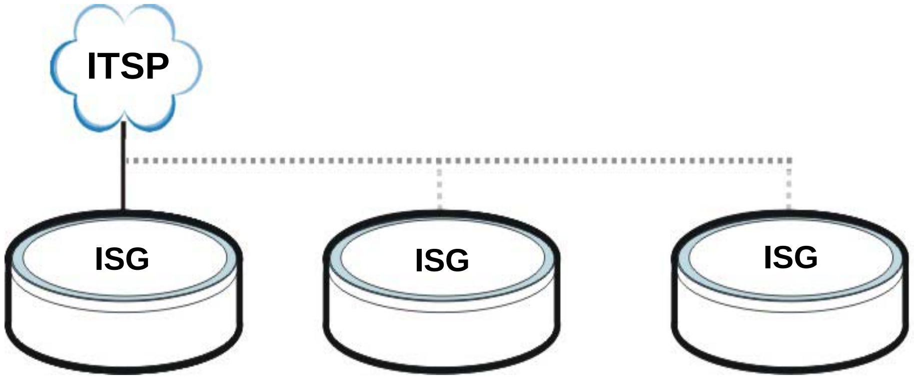
Scalable Design

The ISG50 can be used stand alone to provide intercom (calling by extension) and VoIP features in a small business environment. The ISG50's capability can be expanded by:

- **A** - Adding a USB hard disk to store a greater volume of call records.

- **B** - Connecting several ISG50s together to manage a larger telephone network.

Figure 13 Scalable Design



Automatic Call Distribution

Automatic Call Distribution (ACD) allows you to distribute incoming calls to specific groups of phones connected to your telephone network. Distributed calls can then be sent to individual people based on assigned skill sets. This is known as Skill-Based Routing (SBR). When the ISG50 receives an incoming call, it categorizes the call by “skill”. Next, it assigns the call to the one of the agents associated with that skill. Skills are defined by the ISG50 administrator and constitute a set of rules that work in tandem with the auto-attendant to assign incoming calls to groups of agents.

Click-To-Talk

The Click-To-Talk (CTT) feature allows you to create an HTML link that you can embed on a Web page; a person visiting that web page can click it to connect to one of the ISG50’s extensions.

Mobile Phone Extensions

This feature gives users the freedom to access their telephone extensions anywhere in the world, regardless of the type of telecommunications device they are using: cell phone, VoIP, or landline. The “mobile” aspect that the end user can always be on the move and still receive calls sent to their telephone extension.

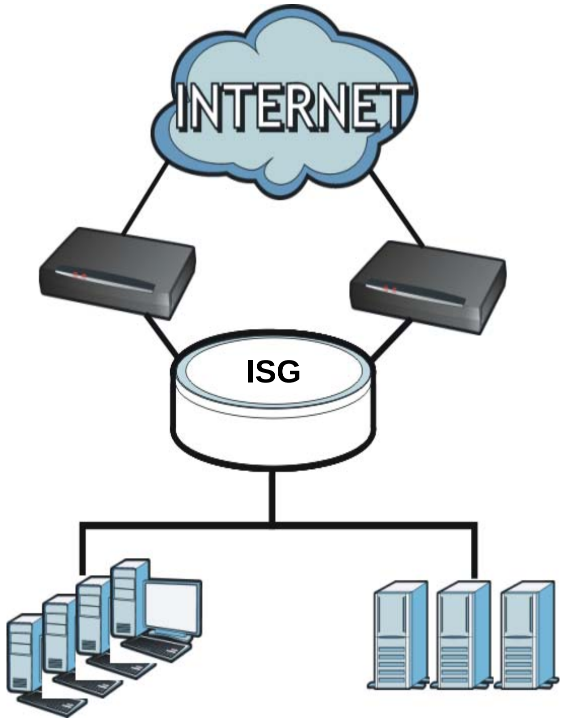
High Availability

To ensure the ISG50 provides reliable, secure Internet access, set up one or more of the following:

- Multiple WAN ports and configure load balancing between these ports.
- A 3G (cellular) connection.

Set up multiple connections to the Internet on the same port, or set up multiple connections on different ports. In either case, you can balance the loads between them.

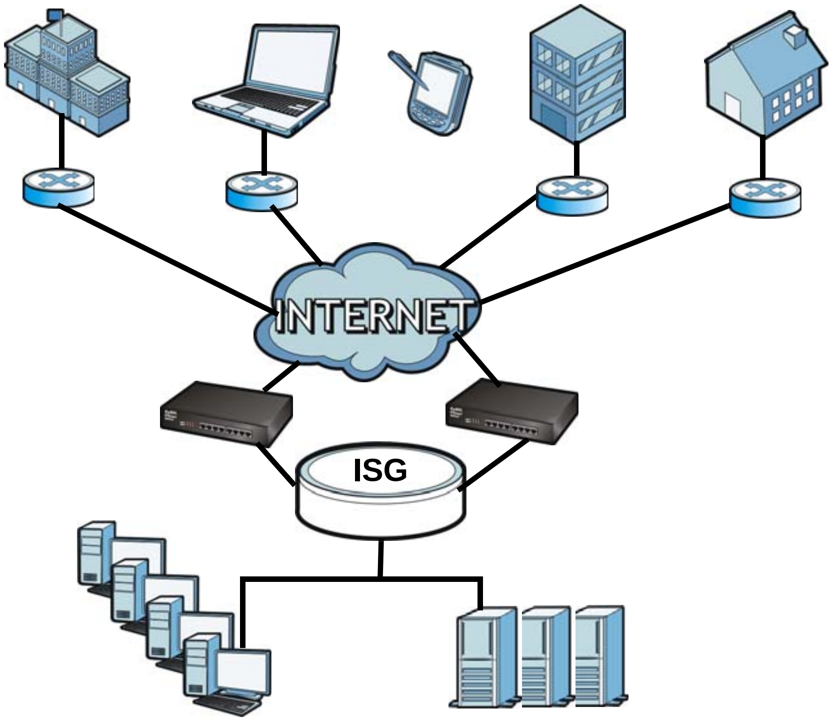
Figure 14 Applications: Multiple WAN Interfaces



Virtual Private Networks (VPN)

Use IPSec VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ISG50 also offers hub-and-spoke IPSec VPN. Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. You can also set up additional connections to the Internet to provide better service.

Figure 15 Applications: VPN Connectivity



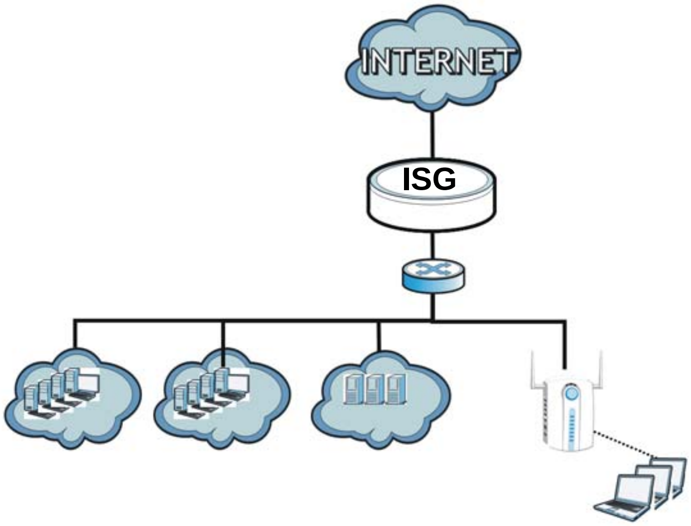
Flexible Security Zones

Many security settings are made by zone, not by interface, port, or network. As a result, it is much simpler to set up and to change security settings in the ISG50. You can create your own custom zones. You can add interfaces and VPN tunnels to zones.

User-Aware Access Control

Set up security policies that restrict access to sensitive information and shared resources based on the user who is trying to access it.

Figure 16 Applications: User-Aware Access Control



Firewall

The ISG50's firewall is a stateful inspection firewall. The ISG50 restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Anomaly Detection and Prevention (ADP)

ADP (Anomaly Detection and Prevention) can detect malicious or suspicious packets and respond instantaneously. It can detect:

- Anomalies based on violations of protocol standards (RFCs – Requests for Comments)
- Abnormal flows such as port scans.

The ISG50's ADP protects against network-based intrusions. See Section 26.3.4 on page 415 and Section 26.3.5 on page 418 for more on the kinds of attacks that the ISG50 can protect against. You can also create your own custom ADP rules.

Bandwidth Management

Bandwidth management allows you to allocate network resources according to defined policies. The ISG50 applies its QoS and queueing to use this policy-based bandwidth allocation to help your network to better handle applications such as Internet access, e-mail, Voice-over-IP (VoIP), video conferencing and other business-critical applications.

3

Web Configurator

The ISG50 Web Configurator allows easy ISG50 setup and management using an Internet browser.

3.1 Web Configurator Requirements

In order to use the Web Configurator, you must

- Use Internet Explorer 7 or later, or Firefox 1.5 or later
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScript (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

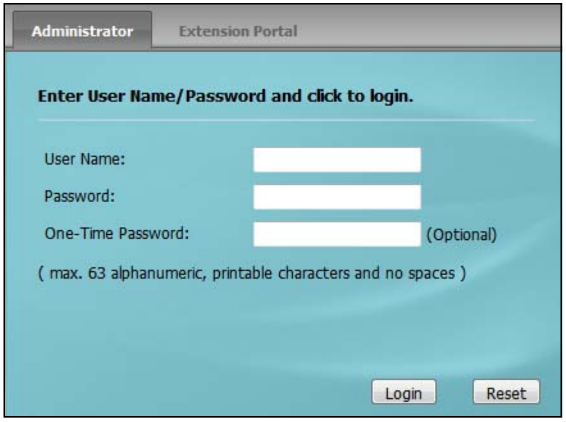
The recommended screen resolution is 1024 x 768 pixels.

3.2 Web Configurator Access

1 Make sure your ISG50 hardware is properly connected. See the Quick Start Guide.

2 Open your web browser, and go to http://192.168.1.1. By default, the ISG50 automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears. To protect against brute force, password-guessing attacks, the ISG50 blocks an account's access for 60 minutes after 3 consecutive, failed login attempts. You can use the commands to change this.

Figure 17 Login Screen



Enter User Name/Password and click to login.

User Name:

Password:

One-Time Password: (Optional)

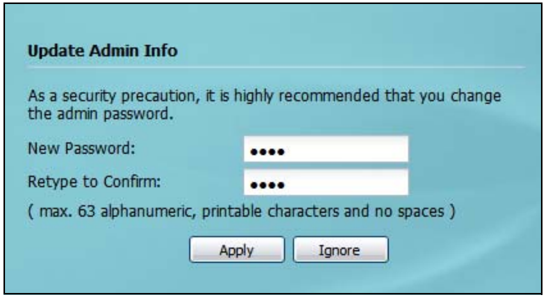
(max. 63 alphanumeric, printable characters and no spaces)

3 Type the user name (default: “admin”) and password (default: “1234”).

If your account is configured to use an ASAS authentication server, use the OTP (One-Time Password) token to generate a number. Enter it in the **One-Time Password** field. The number is only good for one login. You must use the token to generate a new number the next time you log in.

4 Click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen (Figure 18 on page 44) appears. Otherwise, the dashboard (Figure 19 on page 45) appears.

Figure 18 Update Admin Info Screen



Update Admin Info

As a security precaution, it is highly recommended that you change the admin password.

New Password: ••••

Retype to Confirm: ••••

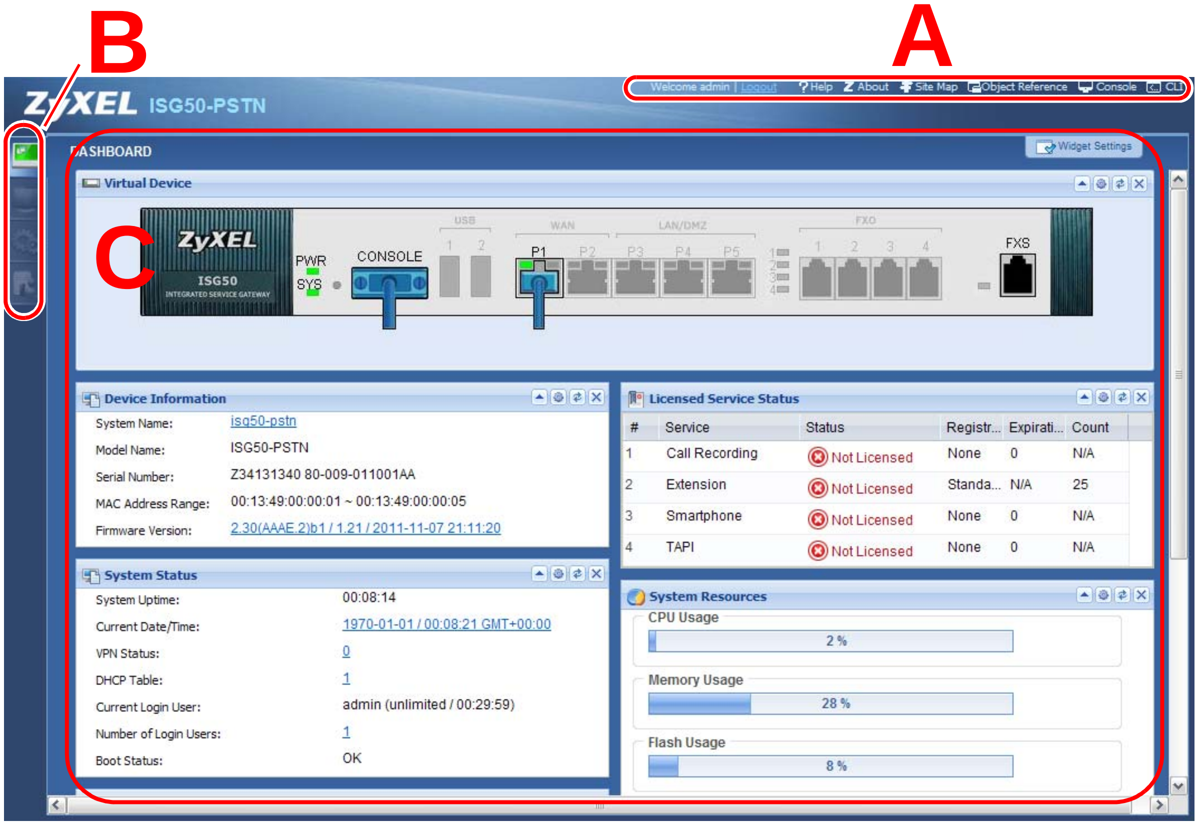
(max. 63 alphanumeric, printable characters and no spaces)

The screen above appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

Follow the directions in this screen. If you change the default password, the **Login** screen (Figure 17 on page 43) appears after you click **Apply**. If you click **Ignore**, the **Installation Setup Wizard** opens if the ISG50 is using its default configuration; otherwise the dashboard appears.

3.3 Web Configurator Screens Overview

Figure 19 Dashboard


A
B
C
ZyXEL ISG50-PSTN
Welcome admin | Logout
Help
About
Site Map
Object Reference
Console
CLI
DASHBOARD
Widget Settings
Virtual Device
ZyXEL
ISG50
INTEGRATED SERVICE GATEWAY
PWR
SYS
CONSOLE
USB
1
2
WAN
P1
LAN/DMZ
P2
P3
P4
P5
FXO
1
2
3
4
FXS
Device Information
System Status
Licensed Service Status
System Resources

System Name: isg50-pstn
Model Name: ISG50-PSTN
Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:13:49:00:00:01 ~ 00:13:49:00:00:05
Firmware Version: 2.30(AAAE.2)b1 / 1.21 / 2011-11-07 21:11:20

System Uptime: 00:08:14
Current Date/Time: 1970-01-01 / 00:08:21 GMT+00:00
VPN Status: 0
DHCP Table: 1
Current Login User: admin (unlimited / 00:29:59)
Number of Login Users: 1
Boot Status: OK

#	Service	Status	Registr...	Expirati...	Count
1	Call Recording	Not Licensed	None	0	N/A
2	Extension	Not Licensed	Standa...	N/A	25
3	Smartphone	Not Licensed	None	0	N/A
4	TAPI	Not Licensed	None	0	N/A

CPU Usage: 2 %
Memory Usage: 28 %
Flash Usage: 8 %

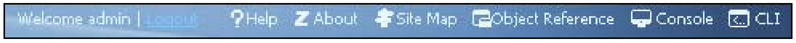
The Web Configurator screen is divided into these parts (as illustrated in Figure 19 on page 45):

- **A** - title bar
- **B** - navigation panel
- **C** - main window

3.3.1 Title Bar

The title bar provides some icons in the upper right corner.

Figure 20 Title Bar


Welcome admin | Logout
Help
About
Site Map
Object Reference
Console
CLI

The icons provide the following functions.

Table 4 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
Help	Click this to open the help page for the current screen.
About	Click this to display basic information about the ISG50.
Site Map	Click this to see an overview of links to the Web Configurator screens.

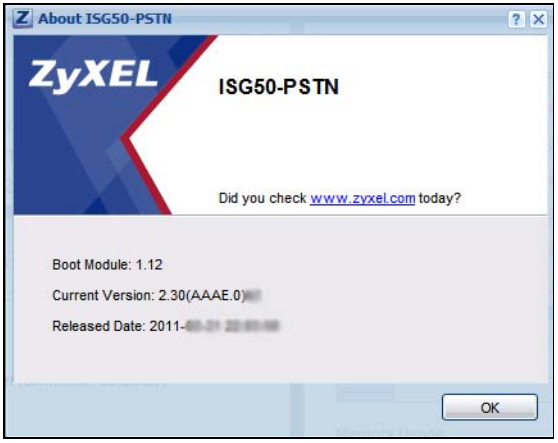
Table 4 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
Object Reference	Click this to open a screen where you can check which configuration items reference an object.
Console	Click this to open the console in which you can use the command line interface (CLI). See the CLI Reference Guide for details on the commands.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator.

3.3.1.1 About

Click this to display basic information about the ISG50.

Figure 21 Title Bar



About ISG50-PSTN

ISG50-PSTN

Did you check www.zyxel.com today?

Boot Module: 1.12

Current Version: 2.30(AAAE.0)[redacted]

Released Date: 2011-[redacted]

The following table describes labels that can appear in this screen.

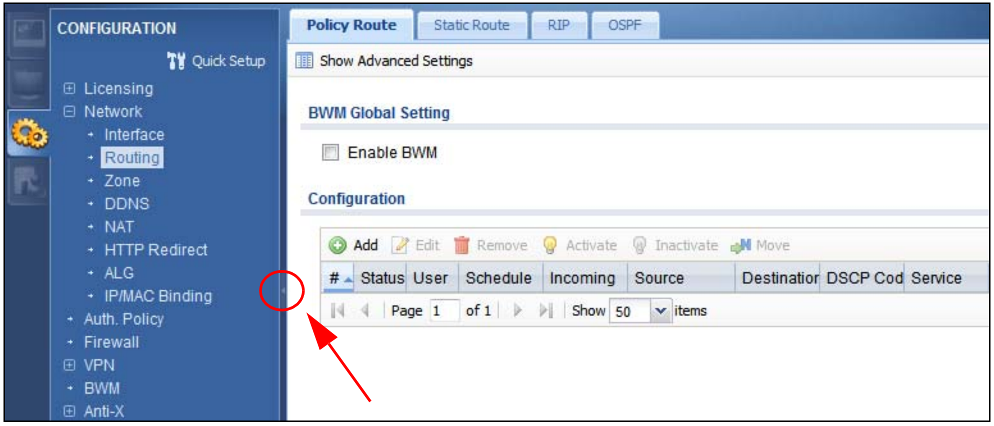
Table 5 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Boot Module	This shows the version number of the software that handles the booting process of the ISG50.
Current Version	This shows the firmware version of the ISG50.
Released Date	This shows the date (yyyy-mm-dd) and time (hh:mm:ss) when the firmware is released.
OK	Click this to close the screen.

3.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ISG50 features. Click the arrow in the middle of the right edge of the navigation panel to hide the navigation panel menus or drag it to resize them. The following sections introduce the ISG50's navigation panel menus and their screens.

Figure 22 Navigation Panel


CONFIGURATION
Quick Setup
Licensing
Network
Interface
Routing
Zone
DDNS
NAT
HTTP Redirect
ALG
IP/MAC Binding
Auth. Policy
Firewall
VPN
BWM
Anti-X
Policy Route
Static Route
RIP
OSPF
Show Advanced Settings
BWM Global Setting
Enable BWM
Configuration
Add
Edit
Remove
Activate
Inactivate
Move
#
Status
User
Schedule
Incoming
Source
Destination
DSCP Cod
Service
Page 1 of 1
Show 50 items

3.3.2.1 Dashboard

The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. See Chapter 9 on page 185 for details on the dashboard.

3.3.2.2 Monitor Menu

The monitor menu screens display status and statistics information.

Table 6 Monitor Menu Screens Summary

FOLDER OR LINK	FUNCTION
System Status	
Port Statistics	Displays packet statistics for each physical port.
Interface Status	Displays general interface information and packet statistics.
Traffic Statistics	Collect and display traffic statistics.
Session Monitor	Displays the status of all current sessions.
DDNS Status	Displays the status of the ISG50's DDNS domain names.
IP/MAC Binding	Lists the devices that have received an IP address from ISG50 interfaces using IP/ MAC binding.
Login Users	Lists the users currently logged into the ISG50.
Cellular Status	Displays details about the ISG50's 3G connection status.
USB Storage	Displays details about USB-connected storage devices.
VPN Monitor	
IPSec	Displays and manages the active IPSec SAs.
PBX	
SIP Peer	Displays status information about SIP extensions configured on the ISG50.
FXS Peer	Displays status information about FXS extensions configured on the ISG50.
SIP Trunk	Displays status information about SIP outbound line groups configured on the ISG50.
CTI Peer	Displays status information about the ISG50's Computer Telephony Integration (CTI) connections.
FXO Trunk	Displays status information about FXO outbound line groups configured on the ISG50.

Table 6 Monitor Menu Screens Summary (continued)

FOLDER OR LINK	FUNCTION
BRI Trunk	Displays status information about ISDN BRI outbound line groups configured on the ISG50.
ACD Queue	Monitor phone call activity for Automatic Call Distribution (ACD) agents.
Log	
System Log	Lists system log entries.
Call Recording	Listen to or delete call recordings on the ISG50.
CDR	Query the CDR database.

3.3.2.3 Configuration Menu

Use the configuration menu screens to configure the ISG50's features.

Table 7 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Quick Setup		Quickly configure WAN interfaces or VPN connections.
Licensing		
Registration	Registration	Register the device and activate trial services.
	Service	View the licensed service status and upgrade licensed services.
Network		
Interface	Port Role	Use this screen to set the ISG50's flexible ports as LAN1 or DMZ.
	Ethernet	Manage Ethernet interfaces and virtual Ethernet interfaces.
	PPP	Create and manage PPPoE and PPTP interfaces.
	Cellular	Configure a cellular Internet connection for an installed 3G card.
	VLAN	Create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Create and manage bridges and virtual bridge interfaces.
	Trunk	Create and manage trunks (groups of interfaces) for load balancing and link High Availability (HA).
Routing	Policy Route	Create and manage routing policies.
	Static Route	Create and manage IP static routing information.
	RIP	Configure device-level RIP settings.
	OSPF	Configure device-level OSPF settings, including areas and virtual links.
Zone		Configure zones used to define various policies.
DDNS		Define and manage the ISG50's DDNS domain names.
NAT		Set up and manage port forwarding rules.
HTTP Redirect		Set up and manage HTTP redirection rules.
ALG		Configure H.323 and FTP pass-through settings.
IP/MAC Binding	Summary	Configure IP to MAC address bindings for devices connected to each supported interface.
	Exempt List	Configure ranges of IP addresses to which the ISG50 does not apply IP/MAC binding.
Auth. Policy		Define rules to force user authentication.
Firewall	Firewall	Create and manage level-3 traffic rules.
	Session Limit	Limit the number of concurrent client NAT/firewall sessions.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
VPN		
IPSec VPN	VPN Connection	Configure IPSec tunnels.
	VPN Gateway	Configure IKE tunnels.
BWM		Control bandwidth for services passing through the ISG50.
Anti-X		
ADP	General	Display and manage ADP bindings.
	Profile	Create and manage ADP profiles.
PBX		
Global	SIP Server	Configure global SIP server settings.
	Feature Code	Set the code users dial on their phone’s keypad to enable or disable a feature the ISG50 supports.
	E-Mail	Configure email settings so users can send voice mails or CDR backup data through the email server.
	Fake IP	Configure settings that may help avoid potential VoIP problems caused be the ISG50 being behind a NAT router.
	Peer to Peer	Set up a direct connection between two IP phones on the same subnet.
	QoS	Configure DSCP settings for SIP or audio traffic.
	TAPI	Configure TAPI line settings and download the ZYXEL TAPI driver.
Voice Interfaces	FXS	Configure settings for the FXS line.
	FXO	Configure settings for the FXO lines.
	BRI	Configure settings for the BRI lines.
Extension Management	Authority Group	Configure and manage the ISG50’s authority groups.
	Group Access Code	Configure a group access code for authority groups.
	Click To Talk	Configure Click-To-Talk (CTT) groups to answer calls sent over the Internet with a web-based IP phone.
Outbound Line Management	Outbound Trunk Group	Configure settings for your outbound line groups.
	Auto-Attendant	Configure the default and customized auto-attendants the ISG50 uses.
	LCR	Configure Least Cost Routing (LCR) dialing rules.
Group Management		Manage the ISG50’s authority groups and outbound line groups.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Call Service	Auto Callback	Automatically call an extension once it becomes available (ends an existing conversation).
	Call Park	Allow users to put a call on hold at one extension and pick up the call from another extension in your organization.
	Call Waiting	Allow users to put a call on hold at one extension and pick up another incoming call.
	Emergency Call	Configure emergency numbers that the ISG50 treats with the highest priority.
	Music On Hold	Upload your choice of audio to play while callers are placed on hold.
	Call Transfer	Allow users to transfer an incoming call that they have answered to another extension in your organization.
	Call Block	Block incoming calls from specific phone numbers or calls without caller ID.
Call Recording		Record calls to or from specific extensions or trunks.
Meet-me Conference		Configure conference room extensions.
Paging Group		Configure sets of extensions through which a caller can broadcast by dialing a single number.
ACD	Global	Configure the the global “wrap up” time for each extension in the Automatic Call Distribution (ACD) system.
	Agent	Manage the ACD agent identities.
	Skill	Manage the ACD skills.
	Hunt Group	Configure a set of extensions that can be reached by dialing a single number. The extensions ring based on a ringing method you configure.
	Skill Menu	Configure menus that a caller can use while in the queue waiting for an agent to respond.
Sound File	System Sound	Select the default language and manage system sound files.
	Specific Sound File	Change a specific sound file.
	Record Peer	Select the peer to record by default.
Auto Provision	Auto Provision	Configure auto provisioning files for your ZyXEL VoIP devices connected to this ISG50.
	Auto Provision Advanced	Configure feature key settings and firmware upgrade URLs for connected snom VoIP devices.
Voice Mail		Configure general and e-mail content settings for voice mail.
Phonebook	General	Select which phonebooks the ISG50 is to use.
	LDAP Phonebook	Imports phonebook entries from an LDAP directory on your network.
	Local Phonebook	Import or export your local phonebook and configure local phonebook entries.
Office Hour		Configure the days of the week and times you are in the office.
Object		
User/Group	User	Create and manage users.
	Group	Create and manage groups of users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Address	Address	Create and manage host, range, and network (subnet) addresses.
	Address Group	Create and manage groups of addresses.
Service	Service	Create and manage TCP and UDP services.
	Service Group	Create and manage groups of services.
Schedule		Create one-time and recurring schedules.
AAA Server	Active Directory	Configure the list of Active Directory servers the ISG50 can use in authenticating users.
	LDAP	Configure the list of LDAP servers the ISG50 can use in authenticating users.
	RADIUS	Configure the list of RADIUS servers the ISG50 can use in authenticating users.
Auth. Method		Create and manage ways of authenticating users.
Certificate	My Certificates	Create and manage the ISG50's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
ISP Account		Create and manage ISP account information for PPPoE/PPTP interfaces.
System		
Host Name		Configure the system and domain name for the ISG50.
USB Storage		Configure the settings for the connected USB devices.
Date/Time		Configure the current date, time, and time zone in the ISG50.
Console Speed		Set the console speed.
DNS		Configure the DNS server and address records for the ISG50.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
	Login Page	Configure how the login and access user screens look.
SSH		Configure SSH server and SSH service settings.
TELNET		Configure telnet server settings for the ISG50.
FTP		Configure FTP server settings.
SNMP		Configure SNMP communities and services.
Language		Select the Web Configurator language.
Log & Report		
Email Daily Report		Configure where and how to send daily reports and what reports to send.
Log Setting		Configure the system log, e-mail logs, and remote syslog servers.
CDR Configuration		Manage CDR collection.

3.3.2.4 Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the ISG50.

Table 8 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the ISG50.
	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the ISG50.
Diagnostics	Diagnostics	Collect diagnostic information.
	Packet Capture	Capture packets for analysis.
	Core Dump	Have the ISG50 save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes).
	System Log	Download files of system logs from a connected USB storage device to your computer.
Packet Flow Explore	Routing Status	View a clear picture on how the ISG50 determines where to route a packet and check the related settings.
	SNAT Status	View a clear picture on how the ISG50 converts a packet's source IP address and check the related settings.
Reboot		Restart the ISG50.
Shutdown		Turn off the ISG50.

3.3.3 Main Window

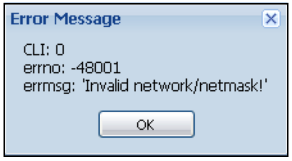
The main window shows the screen you select in the navigation panel. The main window screens are discussed in the rest of this document.

Right after you log in, the **Dashboard** screen is displayed. See Chapter 9 on page 185 for more information about the **Dashboard** screen.

3.3.3.1 Warning Messages

Warning messages, such as those resulting from misconfiguration, display in a popup window.

Figure 23 Warning Message

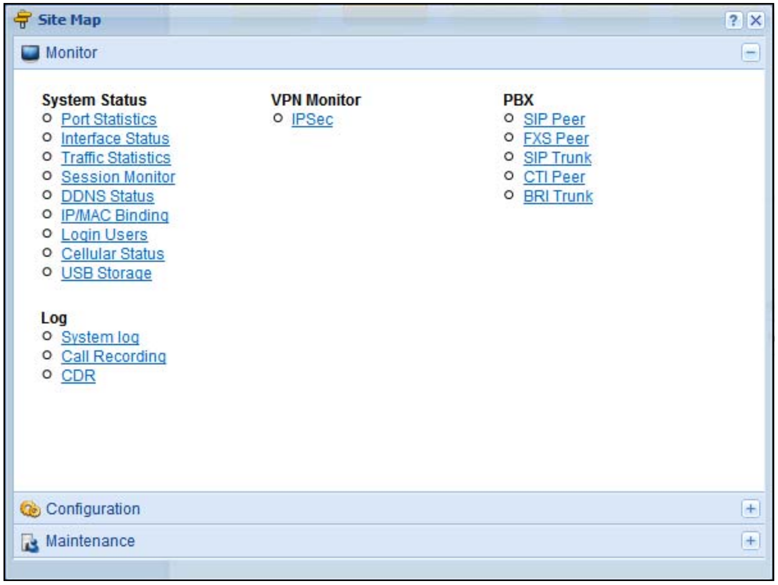


CLI: 0
errno: -48001
errmsg: 'Invalid network/netmask!'

3.3.3.2 Site Map

Click **Site MAP** to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

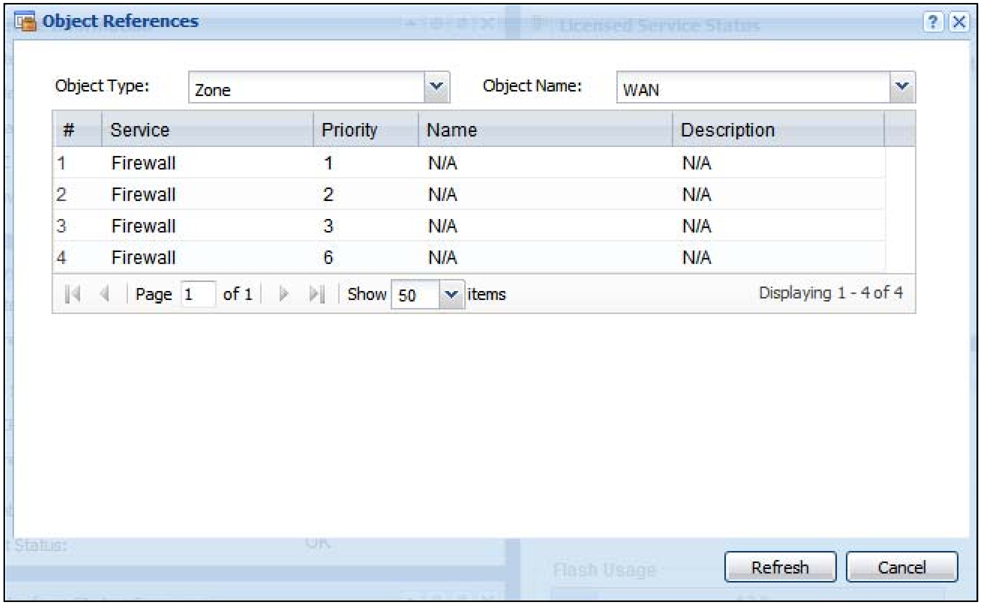
Figure 24 Site Map


Site Map
Monitor
System Status
Port Statistics
Interface Status
Traffic Statistics
Session Monitor
DDNS Status
IP/MAC Binding
Login Users
Cellular Status
USB Storage
VPN Monitor
IPSec
PBX
SIP Peer
FXS Peer
SIP Trunk
CTI Peer
BRI Trunk
Log
System log
Call Recording
CDR
Configuration
Maintenance

3.3.3.3 Object Reference

Click **Object Reference** to open the **Object Reference** screen. Select the type of object and the individual object and click **Refresh** to show which configuration settings reference the object. The following example shows which configuration settings reference the ldap-users user object (in this case the first firewall rule).

Figure 25 Object Reference


Object References

Object Type: Zone

Object Name: WAN

#	Service	Priority	Name	Description
1	Firewall	1	N/A	N/A
2	Firewall	2	N/A	N/A
3	Firewall	3	N/A	N/A
4	Firewall	6	N/A	N/A

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

Refresh
Cancel

The fields vary with the type of object. The following table describes labels that can appear in this screen.

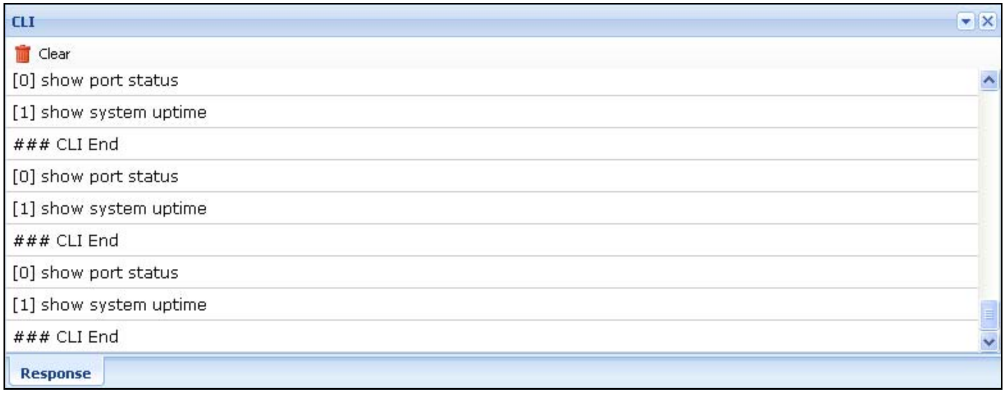
Table 9 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise **N/A** displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click **Cancel** to close the screen.

3.3.3.4 CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. These commands appear in a popup window, such as the following.

Figure 26 CLI Messages



```
[0] show port status
[1] show system uptime
### CLI End
[0] show port status
[1] show system uptime
### CLI End
[0] show port status
[1] show system uptime
### CLI End
```

Click **Clear** to remove the currently displayed information.

See the Command Reference Guide for information about the commands.

3.3.4 Tables and Lists

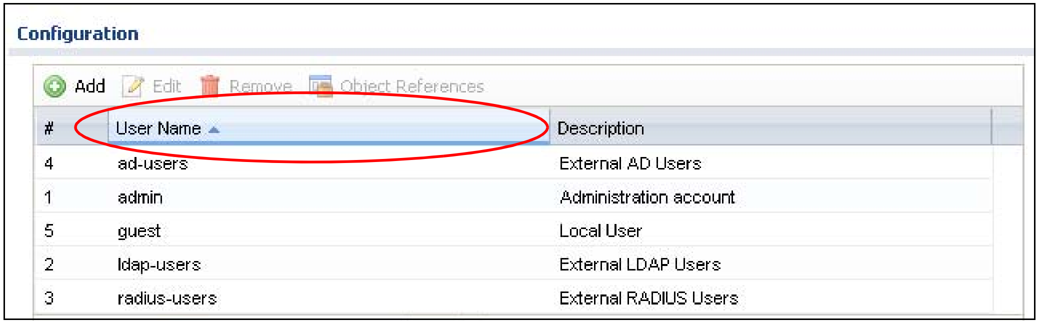
The Web Configurator tables and lists are quite flexible and provide several options for how to display their entries.

3.3.4.1 Manipulating Table Display

Here are some of the ways you can manipulate the Web Configurator tables.

1 Click a column heading to sort the table's entries according to that column's criteria.

Figure 27 Sorting Table Entries by a Column's Criteria

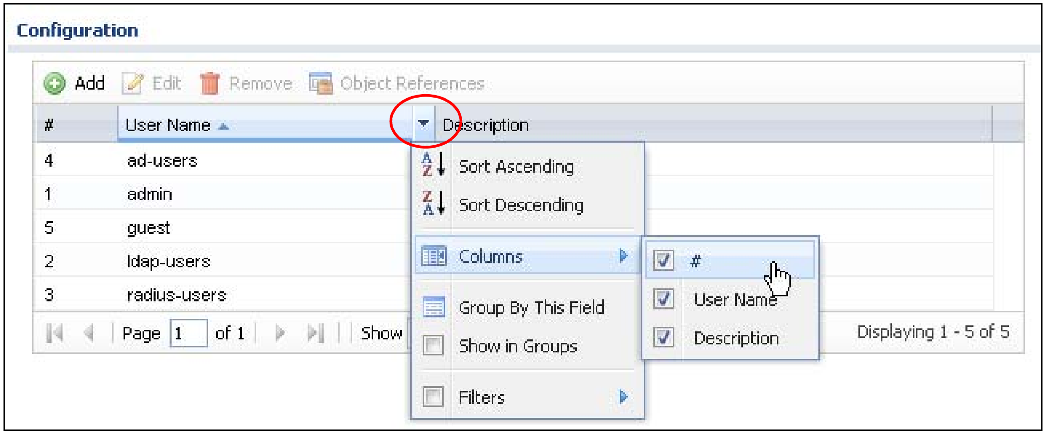

Configuration
Add
Edit
Remove
Object References

#	User Name ▲	Description
4	ad-users	External AD Users
1	admin	Administration account
5	guest	Local User
2	ldap-users	External LDAP Users
3	radius-users	External RADIUS Users

2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

- Sort in ascending alphabetical order
- Sort in descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text

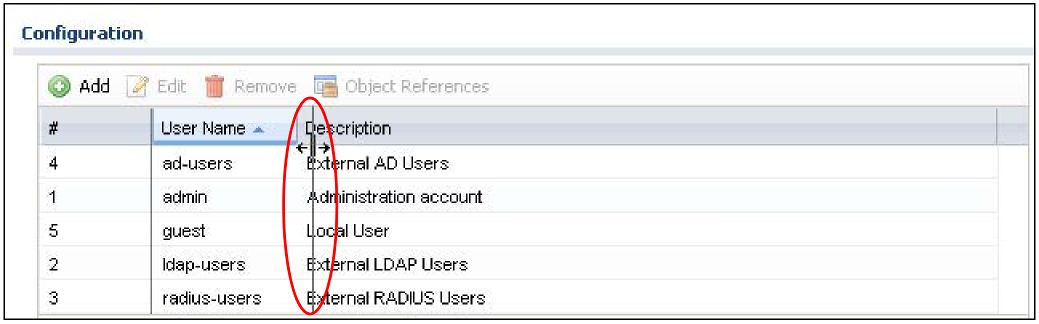
Figure 28 Common Table Column Options


Configuration
Add
Edit
Remove
Object References
Sort Ascending
Sort Descending
Columns
☑ #
☑ User Name
☑ Description
Group By This Field
☐ Show in Groups
☐ Filters
Page 1 of 1
Show
Displaying 1 - 5 of 5

#	User Name ▲	Description
4	ad-users	
1	admin	
5	guest	
2	ldap-users	
3	radius-users	

3 Select a column heading cell's right border and drag to re-size the column.

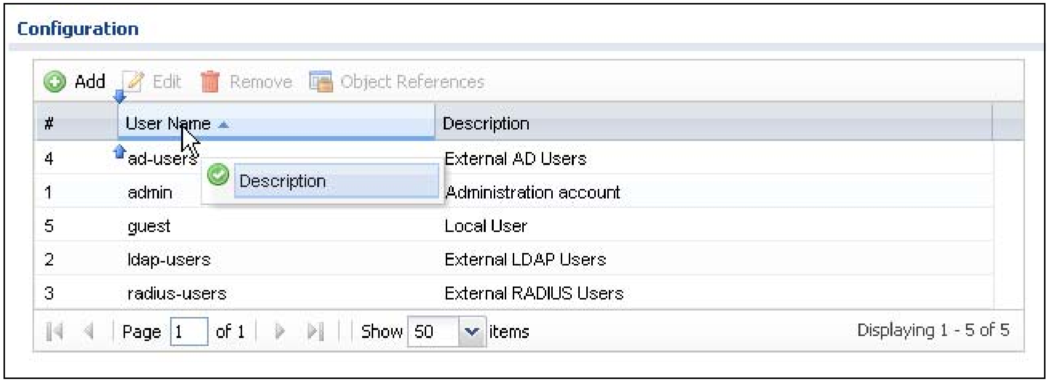
Figure 29 Resizing a Table Column


Configuration
Add
Edit
Remove
Object References

#	User Name ▲	Description
4	ad-users	External AD Users
1	admin	Administration account
5	guest	Local User
2	ldap-users	External LDAP Users
3	radius-users	External RADIUS Users

4 Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

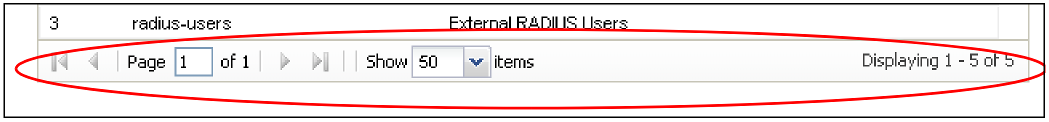
Figure 30 Changing the Column Order


Configuration
Add
Edit
Remove
Object References
Description
Page 1 of 1
Show 50 items
Displaying 1 - 5 of 5

#	User Name	Description
4	ad-users	External AD Users
1	admin	Administration account
5	guest	Local User
2	ldap-users	External LDAP Users
3	radius-users	External RADIUS Users

5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.

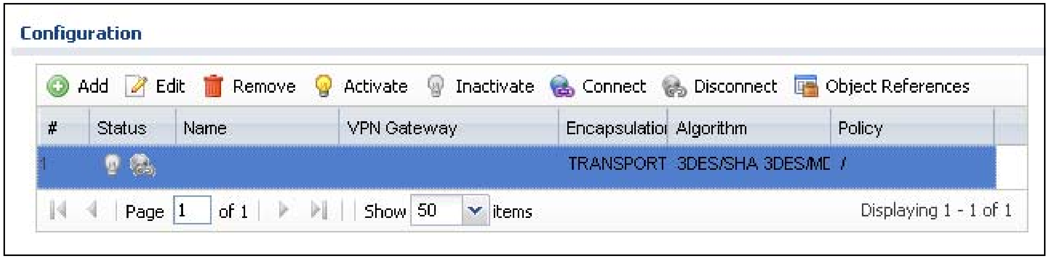
Figure 31 Navigating Pages of Table Entries


3
radius-users
External RADIUS Users
Page 1 of 1
Show 50 items
Displaying 1 - 5 of 5

3.3.4.2 Working with Table Entries

The tables have icons for working with table entries. A sample is shown next. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

Figure 32 Common Table Icons


Configuration
Add
Edit
Remove
Activate
Inactivate
Connect
Disconnect
Object References
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1

#	Status	Name	VPN Gateway	Encapsulatioı	Algorithm	Policy
1				TRANSPORT	3DES/SHA 3DES/MC	/

Here are descriptions for the most common table icons.

Table 10 Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the ISG50 applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.

Table 10 Common Table Icons (continued)

LABEL	DESCRIPTION
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an entry, select it and click **Connect**.
Disconnect	To disconnect an entry, select it and click **Disconnect**.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
Move	To change an entry's position in a numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one.

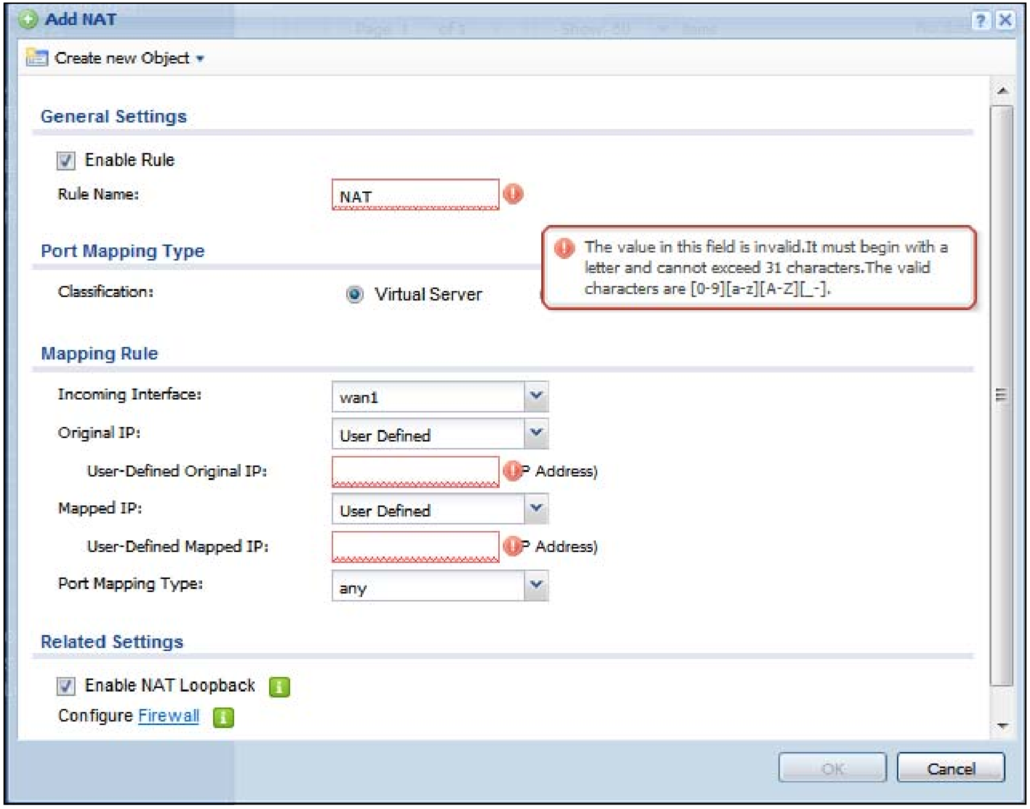
3.3.4.3 Working with Lists

When a list of available entries displays next to a list of selected entries, you can often just double-click an entry to move it from one list to the other. In some lists you can also use the [Shift] or [Ctrl] key to select multiple entries, and then use the arrow button to move them to the other list.

3.3.4.4 Field Input Warnings

For some fields a red dot exclamation point icon displays if you have not entered a valid value. Hover your cursor over the icon for details.

Figure 33 Field Information



☑ Enable Rule

Rule Name: NAT

The value in this field is invalid.It must begin with a letter and cannot exceed 31 characters.The valid characters are [0-9][a-z][A-Z][_-].

Classification: ● Virtual Server

Incoming Interface: wan1

Original IP: User Defined

User-Defined Original IP: P Address)

Mapped IP: User Defined

User-Defined Mapped IP: P Address)

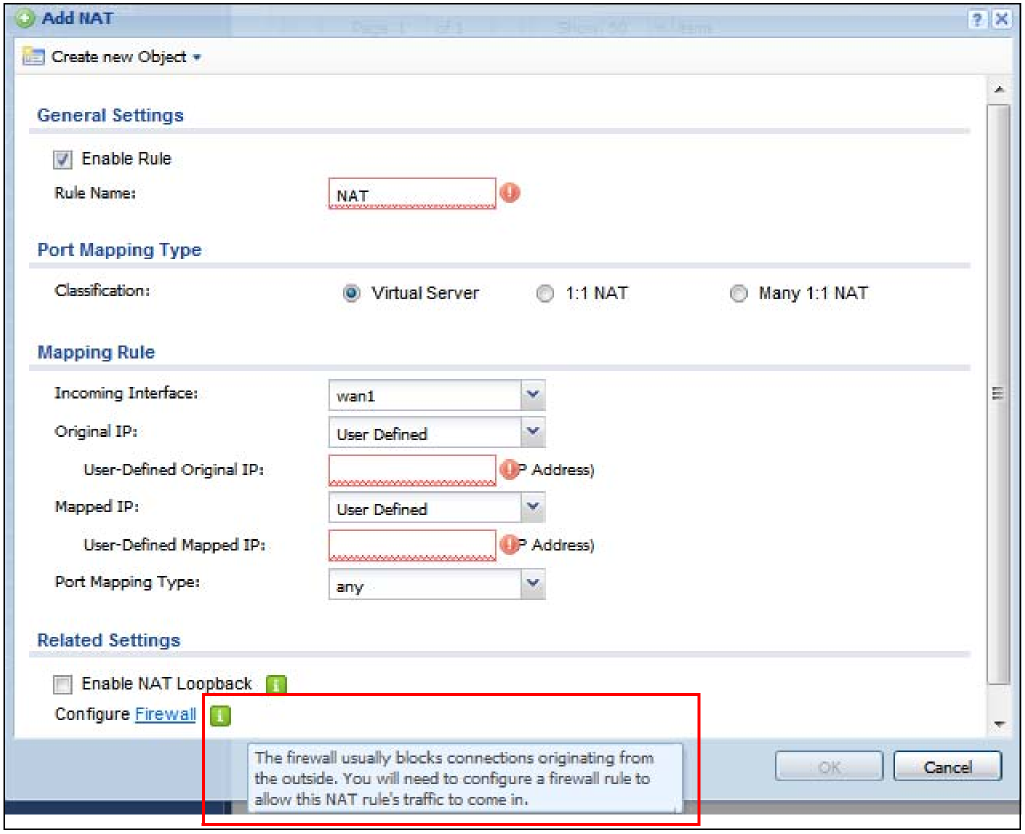
Port Mapping Type: any

☑ Enable NAT Loopback

3.3.4.5 iNotes

The iNote icon is a green square with an ‘i’. Hover your cursor over the icon to display information.

Figure 34 iNotes


Add NAT
Create new Object
General Settings
Port Mapping Type
Mapping Rule
Related Settings
OK
Cancel

☑ Enable Rule
Rule Name: NAT
Classification: ● Virtual Server ○ 1:1 NAT ○ Many 1:1 NAT
Incoming Interface: wan1
Original IP: User Defined
User-Defined Original IP: P Address)
Mapped IP: User Defined
User-Defined Mapped IP: P Address)
Port Mapping Type: any
☐ Enable NAT Loopback
Configure Firewall

The firewall usually blocks connections originating from the outside. You will need to configure a firewall rule to allow this NAT rule's traffic to come in.

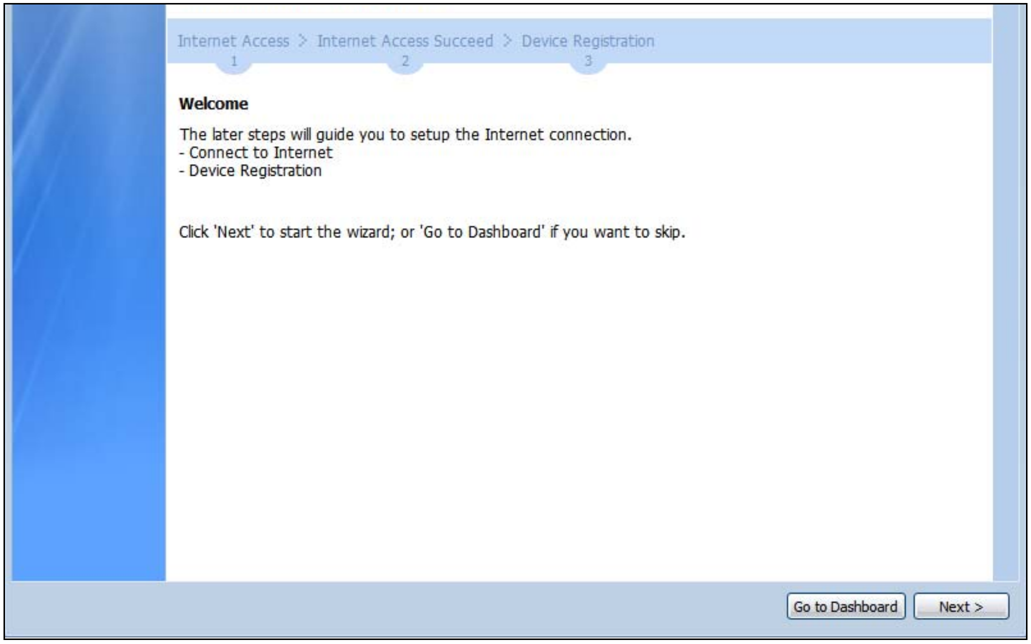
4

Installation Setup Wizard

4.1 Installation Setup Wizard Screens

If you log into the Web Configurator when the ISG50 is using its default configuration, the first **Installation Setup Wizard** screen displays. This wizard helps you configure Internet connection settings and activate subscription services. This chapter provides information on configuring the Web Configurator's installation setup wizard. See the feature-specific chapters in this User's Guide for background information.

Figure 35 Installation Setup Wizard



Welcome

The later steps will guide you to setup the Internet connection.
- Connect to Internet
- Device Registration

Click 'Next' to start the wizard; or 'Go to Dashboard' if you want to skip.

- Click the double arrow in the upper right corner to display or hide the help.
- Click **Go to Dashboard** to skip the installation setup wizard or click **Next** to start configuring for Internet access.

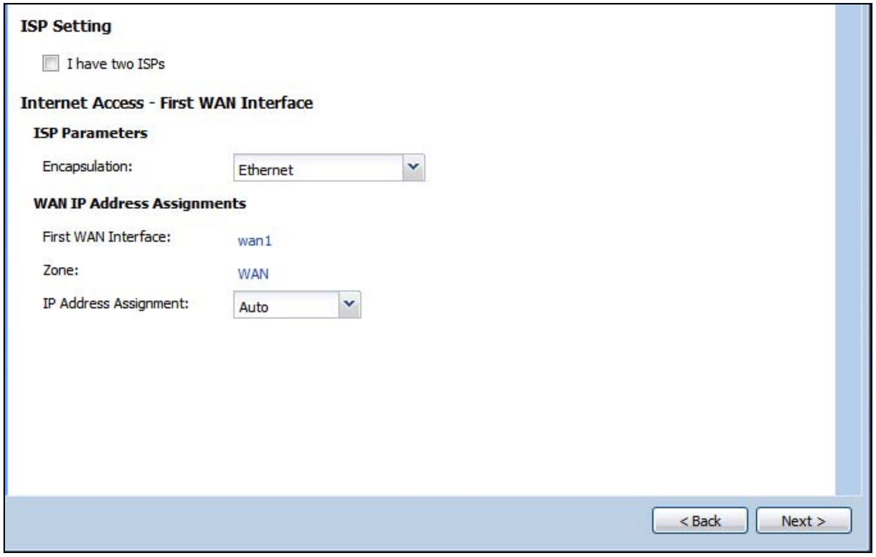
4.1.1 Internet Access Setup - WAN Interface

Use this screen to set how many WAN interfaces to configure and the first WAN interface's type of encapsulation and method of IP address assignment.

The screens vary depending on the encapsulation type. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

Figure 36 Internet Access: Step 1



ISP Setting

☐ I have two ISPs

Internet Access - First WAN Interface

ISP Parameters

Encapsulation: Ethernet

WAN IP Address Assignments

First WAN Interface: wan1

Zone: WAN

IP Address Assignment: Auto

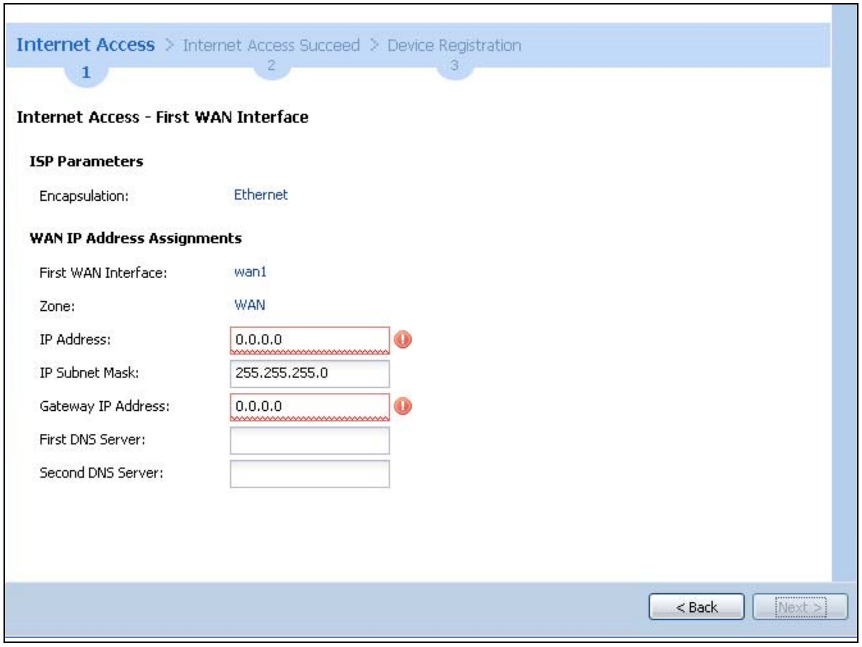
- **I have two ISPs**: Select this option to configure two Internet connections. Leave it cleared to configure just one. This option appears when you are configuring the first WAN interface.
- **Encapsulation**: Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPP over Ethernet** or **PPTP** for a dial-up connection according to the information from your ISP.
- **WAN Interface**: This is the interface you are configuring for Internet access.
- **Zone**: This is the security zone to which this interface and Internet connection belong.
- **IP Address Assignment**: Select **Auto** if your ISP did not assign you a fixed IP address. Select **Static** if the ISP assigned a fixed IP address.

4.1.2 Internet Access: Ethernet

This screen is read-only if you set the previous screen's **IP Address Assignment** field to **Auto**. Use this screen to configure your IP address settings.

Note: Enter the Internet access information exactly as given to you by your ISP.

Figure 37 Internet Access: Ethernet Encapsulation


Internet Access > Internet Access Succeed > Device Registration
1
2
3

Internet Access - First WAN Interface

ISP Parameters

Encapsulation: Ethernet

WAN IP Address Assignments

First WAN Interface: wan1

Zone: WAN

IP Address: 0.0.0.0

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

First DNS Server:

Second DNS Server:

- **Encapsulation**: This displays the type of Internet connection you are configuring.
- **First WAN Interface**: This is the number of the interface that will connect with your ISP.
- **Zone:** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.

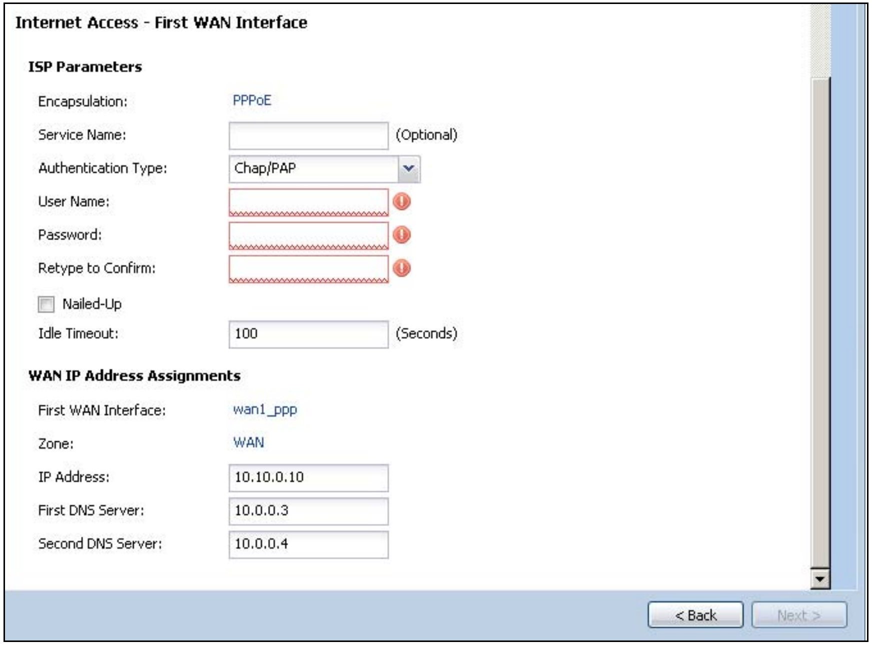
The following fields display if you selected static IP address assignment.

- **IP Subnet Mask**: Enter the subnet mask for this WAN connection's IP address.
- **Gateway IP Address**: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).
- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ISG50 uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

4.1.3 Internet Access: PPPoE

Note: Enter the Internet access information exactly as given to you by your ISP.

Figure 38 Internet Access: PPPoE Encapsulation



Internet Access - First WAN Interface

ISP Parameters

Encapsulation: PPPoE

Service Name: (Optional)

Authentication Type: Chap/PAP

User Name:

Password:

Retype to Confirm:

☐ Nailed-Up

Idle Timeout: 100 (Seconds)

WAN IP Address Assignments

First WAN Interface: wan1_ppp

Zone: WAN

IP Address: 10.10.0.10

First DNS Server: 10.0.0.3

Second DNS Server: 10.0.0.4

4.1.3.1 ISP Parameters

- Type the PPPoE **Service Name** from your service provider. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@$./ characters, and it can be up to 64 characters long.
- **Authentication Type** - Select an authentication protocol for outgoing connection requests. Options are:
  - **CHAP/PAP** - Your ISG50 accepts either CHAP or PAP when requested by the remote node.
  - **CHAP** - Your ISG50 accepts CHAP only.
  - **PAP** - Your ISG50 accepts PAP only.
  - **MSCHAP** - Your ISG50 accepts MSCHAP only.
  - **MSCHAP-V2** - Your ISG50 accepts MSCHAP-V2 only.
- Type the **User Name** given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Type the **Password** associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
- Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPPoE server.

4.1.3.2 WAN IP Address Assignments

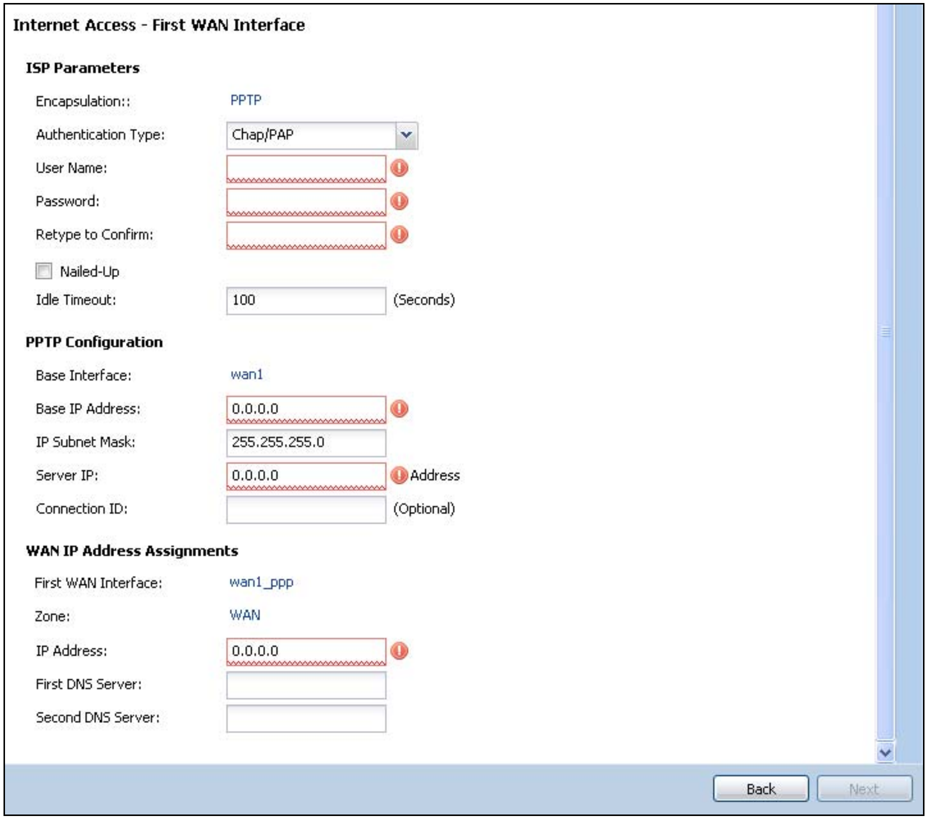
- **WAN Interface**: This is the name of the interface that will connect with your ISP.
- **Zone:** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.

- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ISG50 uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

4.1.4 Internet Access: PPTP

Note: Enter the Internet access information exactly as given to you by your ISP.

Figure 39 Internet Access: PPTP Encapsulation



Internet Access - First WAN Interface

ISP Parameters

Encapsulation:: PPTP
Authentication Type: Chap/PAP
User Name:
Password:
Retype to Confirm:
☐ Nailed-Up
Idle Timeout: 100 (Seconds)

PPTP Configuration

Base Interface: wan1
Base IP Address: 0.0.0.0
IP Subnet Mask: 255.255.255.0
Server IP: 0.0.0.0 Address
Connection ID: (Optional)

WAN IP Address Assignments

First WAN Interface: wan1_ppp
Zone: WAN
IP Address: 0.0.0.0
First DNS Server:
Second DNS Server:

4.1.5 ISP Parameters

- **Authentication Type** - Select an authentication protocol for outgoing calls. Options are:
  - **CHAP/PAP** - Your ISG50 accepts either CHAP or PAP when requested by the remote node.
  - **CHAP** - Your ISG50 accepts CHAP only.
  - **PAP** - Your ISG50 accepts PAP only.
  - **MSCHAP** - Your ISG50 accepts MSCHAP only.
  - **MSCHAP-V2** - Your ISG50 accepts MSCHAP-V2 only.
- Type the **User Name** given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Type the **Password** associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank. Re-type your password in the next field to confirm it.

- Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPTP server.

4.1.5.1 PPTP Configuration

- **Base Interface**: This identifies the Ethernet interface you configure to connect with a modem or router.
- Type a **Base IP Address** (static) assigned to you by your ISP.
- Type the **IP Subnet Mask** assigned to you by your ISP (if given).
- **Server IP**: Type the IP address of the PPTP server.
- Type a **Connection ID** or connection name. It must follow the “c:id” and “n:name” format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your broadband modem or router. You can use alphanumeric and **-_:** characters, and it can be up to 31 characters long.

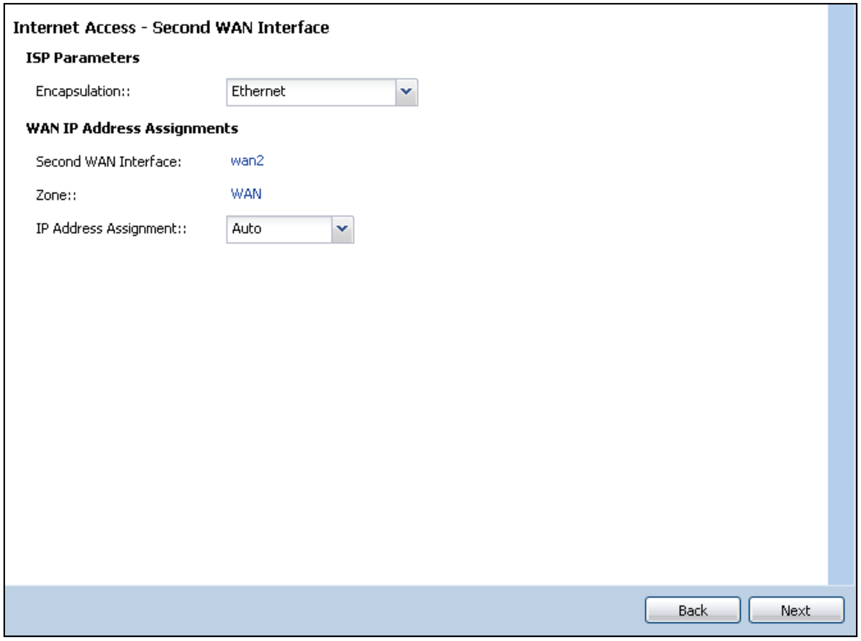
4.1.5.2 WAN IP Address Assignments

- **First WAN Interface**: This is the connection type on the interface you are configuring to connect with your ISP.
- **Zone** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. Auto displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.
- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ISG50 uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

4.1.6 Internet Access Setup - Second WAN Interface

If you selected **I have two ISPs**, after you configure the **First WAN Interface**, you can configure the **Second WAN Interface**. The screens for configuring the second WAN interface are similar to the first (see Section 4.1.1 on page 59).

Figure 40 Internet Access: Step 3: Second WAN Interface



Internet Access - Second WAN Interface

ISP Parameters

Encapsulation:: Ethernet

WAN IP Address Assignments

Second WAN Interface: wan2

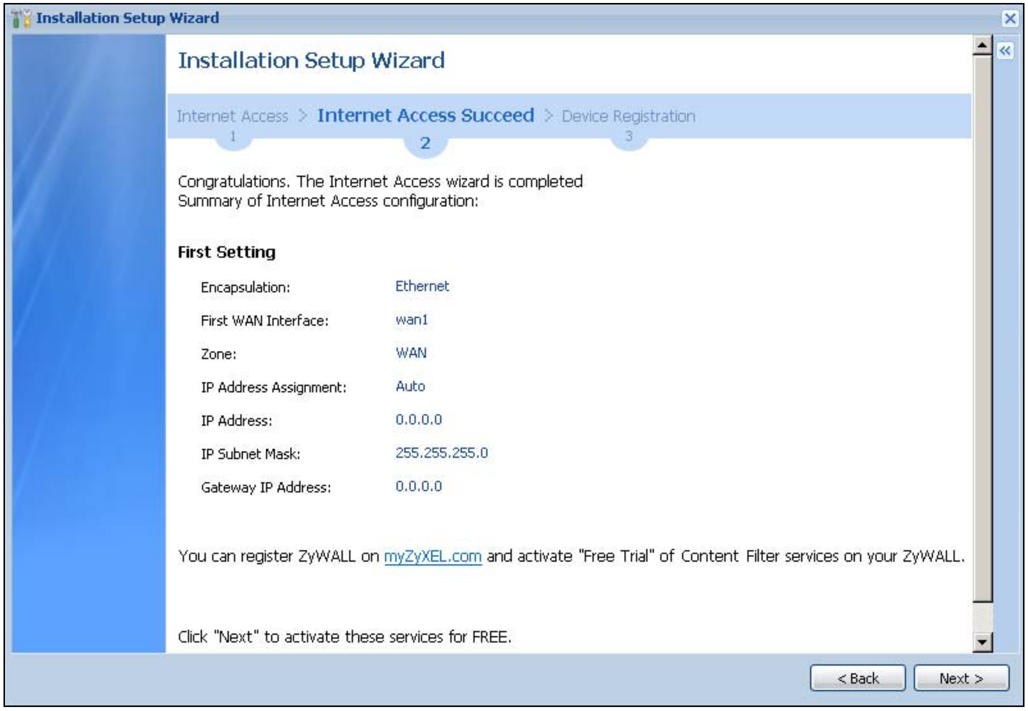
Zone:: WAN

IP Address Assignment:: Auto

4.1.7 Internet Access - Finish

You have set up your ISG50 to access the Internet. After configuring the WAN interface(s), a screen displays with your settings. If they are not correct, click **Back**.

Figure 41 Internet Access: Ethernet Encapsulation



Installation Setup Wizard
Installation Setup Wizard
Internet Access 1
Internet Access Succeed 2
Device Registration 3

Congratulations. The Internet Access wizard is completed
Summary of Internet Access configuration:

First Setting

Encapsulation: Ethernet
First WAN Interface: wan1
Zone: WAN
IP Address Assignment: Auto
IP Address: 0.0.0.0
IP Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0

You can register ZyWALL on myZyXEL.com and activate "Free Trial" of Content Filter services on your ZyWALL.

Click "Next" to activate these services for FREE.

Note: If you have not already done so, you can register your ISG50 with myZyXEL.com.

Click **Next** and use the following screen to perform a basic registration (see Section 4.2 on page 66). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, close the window to exit the wizard.

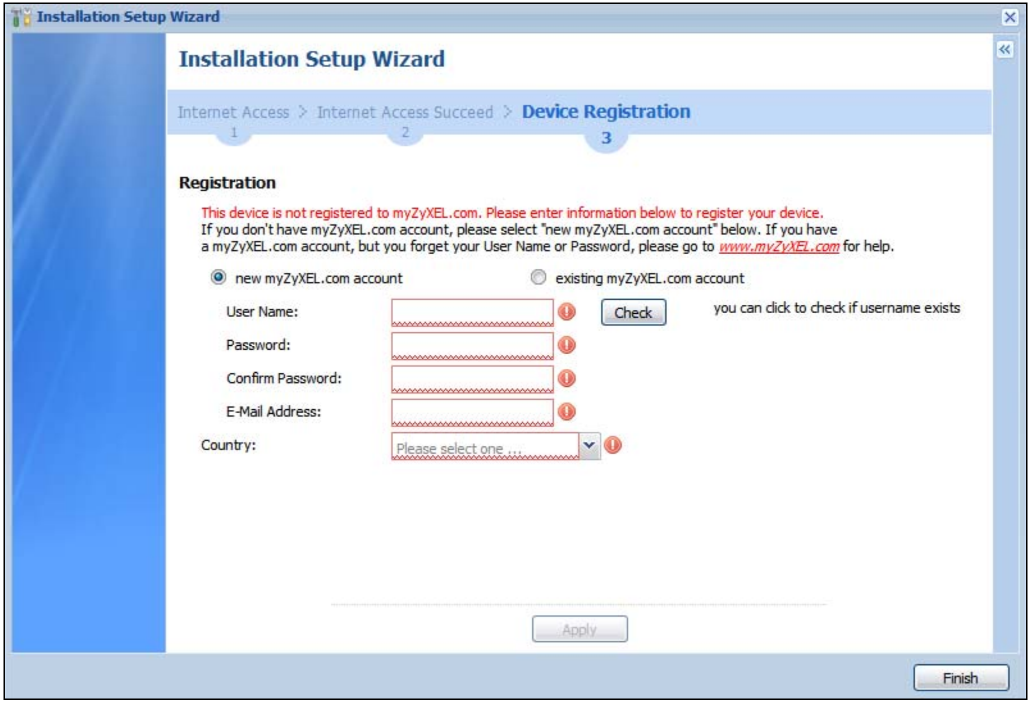
4.2 Device Registration

Use this screen to register your ISG50 with myZXEL.com and activate trial periods of subscription security features if you have not already done so. If the ISG50 is already registered this screen displays your user name and which trial services are activated (if any). You can still activate any un-activated trial services.

Note: You must be connected to the Internet to register.

Use the **Registration > Service** screen to update your service subscription status.

Figure 42 Registration



Installation Setup Wizard
Installation Setup Wizard
Internet Access 1 > Internet Access Succeed 2 > Device Registration 3
Registration

This device is not registered to myZyXEL.com. Please enter information below to register your device.
If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have a myZyXEL.com account, but you forget your User Name or Password, please go to www.myZyXEL.com for help.

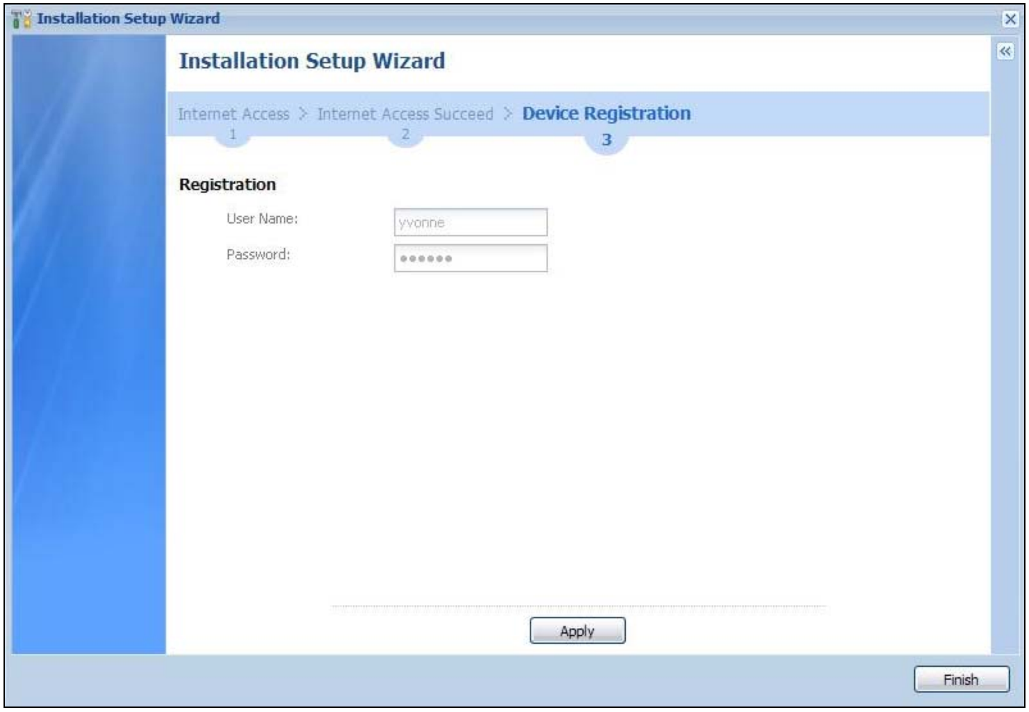
● new myZyXEL.com account ○ existing myZyXEL.com account

User Name: Check — you can click to check if username exists
Password:
Confirm Password:
E-Mail Address:
Country: Please select one ...

- Select **new myZyXEL.com account** if you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ISG50.
- Select **existing myZyXEL.com account** if you already have an account at myZyXEL.com and enter your user name and password in the fields below to register your ISG50.
- Enter a **User Name** for your myZyXEL.com account. Use from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. Click **Check** to verify that it is available.
- **Password**: Use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. Type it again in the **Confirm Password** field.
- **E-Mail Address**: Enter your e-mail address. Use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.

- **Country Code**: Select your country from the drop-down box list.

Figure 43 Registration: Registered Device



Installation Setup Wizard
Installation Setup Wizard
Internet Access > Internet Access Succeed > Device Registration
1
2
3
Registration

User Name: yvonne

Password: ••••••

Apply
Finish

5

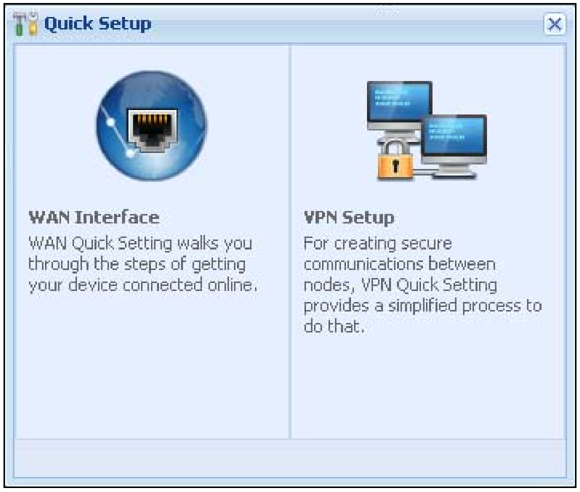
Quick Setup

5.1 Quick Setup Overview

The Web Configurator's quick setup wizards help you configure Internet and VPN connection settings. This chapter provides information on configuring the quick setup screens in the Web Configurator. See the feature-specific chapters in this User's Guide for background information.

In the Web Configurator, click **Configuration > Quick Setup** to open the first **Quick Setup** screen.

Figure 44 Quick Setup



WAN Interface

WAN Quick Setting walks you through the steps of getting your device connected online.

VPN Setup

For creating secure communications between nodes, VPN Quick Setting provides a simplified process to do that.

- **WAN Interface**

  Click this link to open a wizard to set up a WAN (Internet) connection. This wizard creates matching ISP account settings in the ISG50 if you use PPPoE or PPTP. See Section 5.2 on page 70.

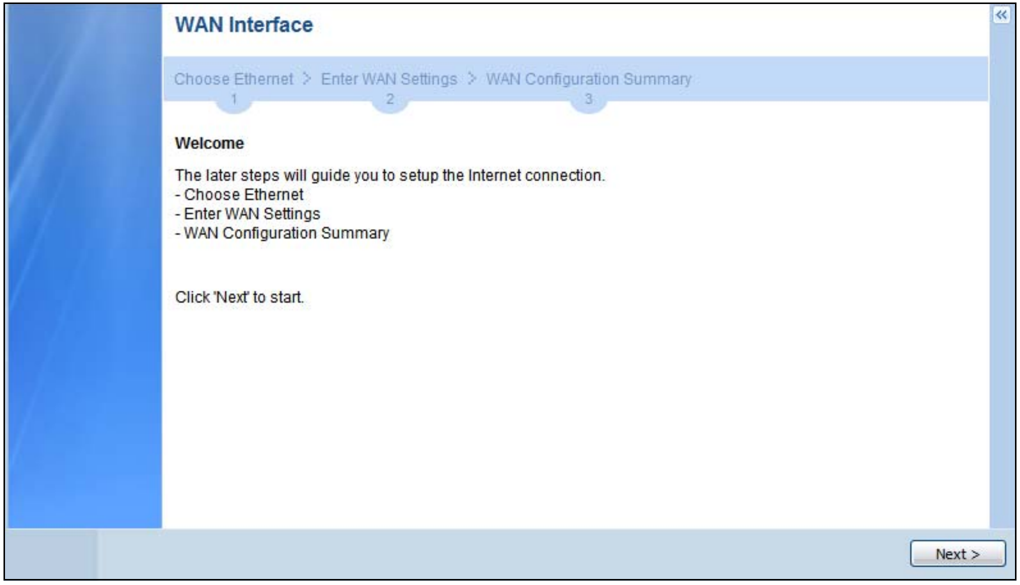
- **VPN SETUP**

  Use **VPN SETUP** to configure a VPN (Virtual Private Network) tunnel for a secure connection to another computer, smartphone, or network. See Section 5.4 on page 77.

5.2 WAN Interface Quick Setup

Click **WAN Interface** in the main **Quick Setup** screen to open the **WAN Interface Quick Setup Wizard Welcome** screen. Use these screens to configure an interface to connect to the internet. Click **Next**.

Figure 45 WAN Interface Quick Setup Wizard



WAN Interface
Choose Ethernet 1
Enter WAN Settings 2
WAN Configuration Summary 3
Next >

Welcome

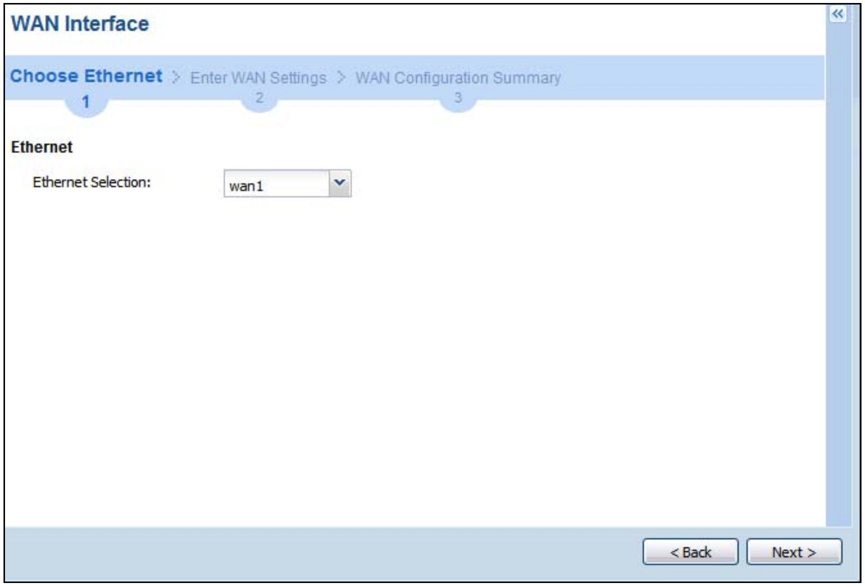
The later steps will guide you to setup the Internet connection.
- Choose Ethernet
- Enter WAN Settings
- WAN Configuration Summary

Click 'Next' to start.

5.2.1 Choose an Ethernet Interface

Select the Ethernet interface that you want to configure for a WAN connection and click **Next**.

Figure 46 Choose an Ethernet Interface



WAN Interface
Choose Ethernet 1
Enter WAN Settings 2
WAN Configuration Summary 3
< Back
Next >

Ethernet

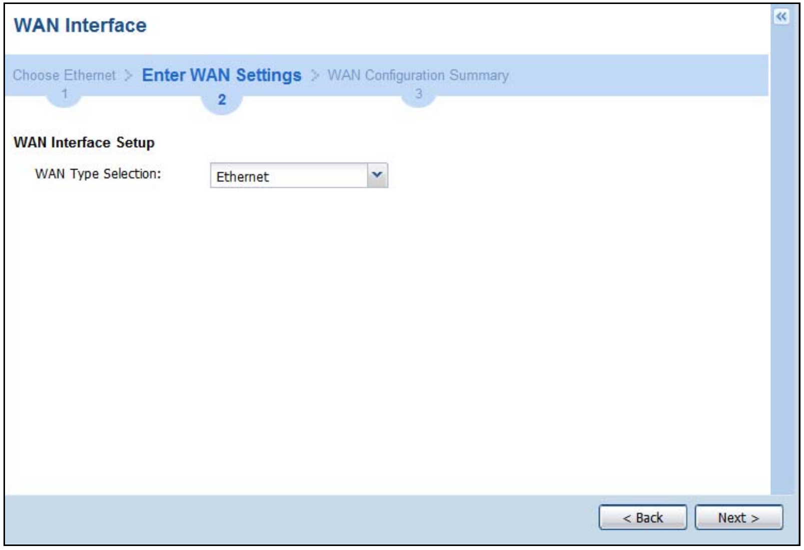
Ethernet Selection: wan1

5.2.2 Select WAN Type

WAN Type Selection: Select the type of encapsulation this connection is to use. Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.

Figure 47 WAN Interface Setup: Step 2



WAN Interface
Choose Ethernet
1
Enter WAN Settings
2
WAN Configuration Summary
3
WAN Interface Setup
< Back
Next >

WAN Type Selection: Ethernet

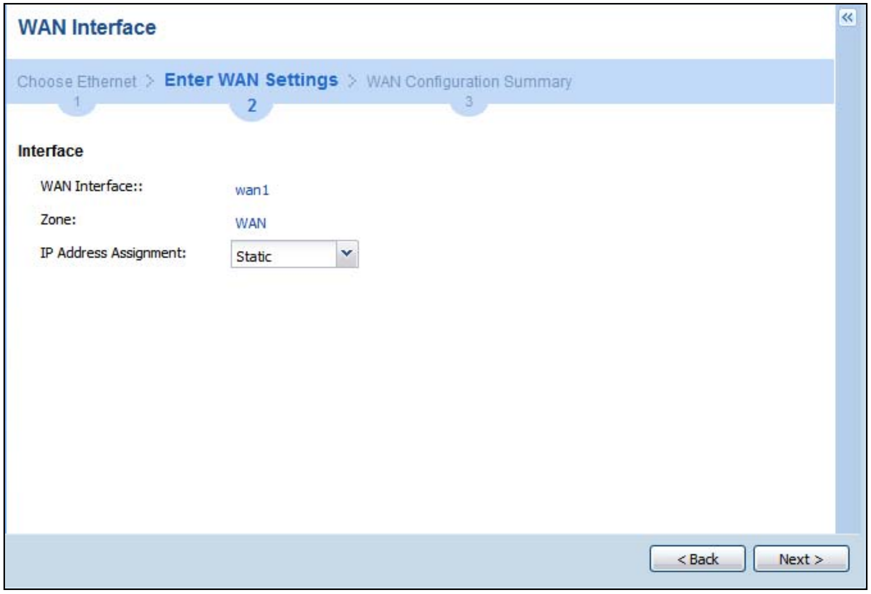
The screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

5.2.3 Configure WAN Settings

Use this screen to select whether the interface should use a fixed or dynamic IP address.

Figure 48 WAN Interface Setup: Step 2


WAN Interface
Choose Ethernet 1
Enter WAN Settings 2
WAN Configuration Summary 3
< Back
Next >

Interface

WAN Interface:: wan1

Zone: WAN

IP Address Assignment: Static

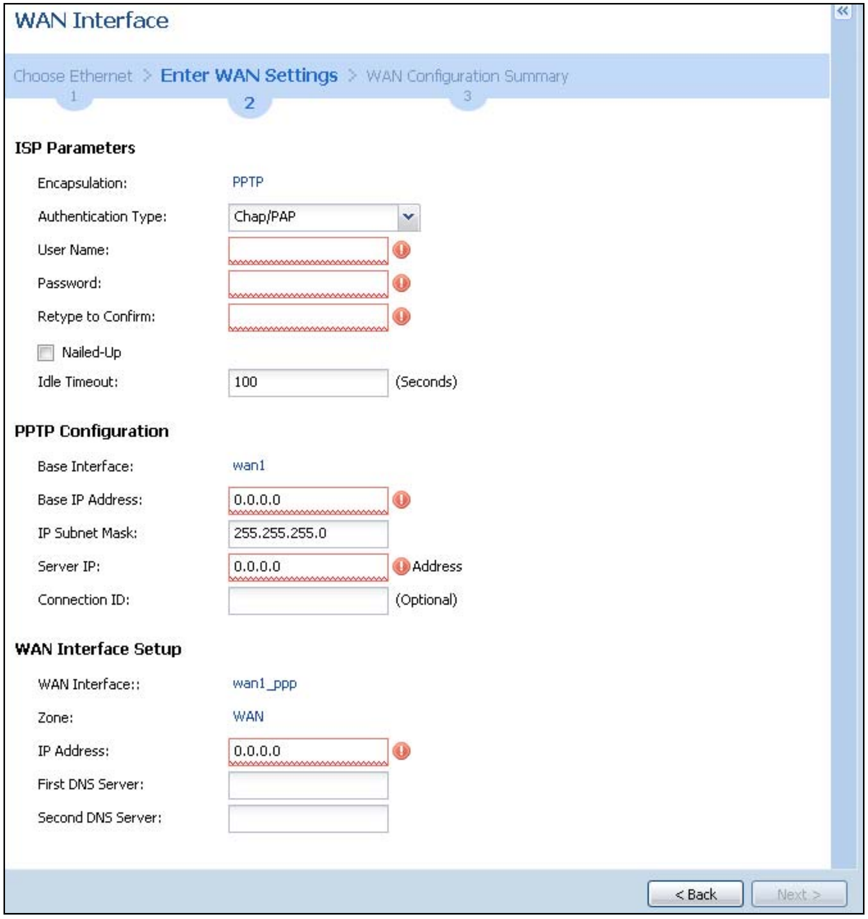
- **WAN Interface**: This is the interface you are configuring for Internet access.
- **Zone**: This is the security zone to which this interface and Internet connection belong.
- **IP Address Assignment**: Select **Auto** If your ISP did not assign you a fixed IP address. Select **Static** If the ISP assigned a fixed IP address.

5.2.4 WAN and ISP Connection Settings

Use this screen to configure the ISP and WAN interface settings. This screen is read-only if you set the **IP Address Assignment** to **Static**.

Note: Enter the Internet access information exactly as your ISP gave it to you.

Figure 49 WAN and ISP Connection Settings: (PPTP Shown)



ISP Parameters

Encapsulation: PPTP

Authentication Type: Chap/PAP

User Name:

Password:

Retype to Confirm:

☐ Nailed-Up

Idle Timeout: 100 (Seconds)

PPTP Configuration

Base Interface: wan1

Base IP Address: 0.0.0.0

IP Subnet Mask: 255.255.255.0

Server IP: 0.0.0.0 Address

Connection ID: (Optional)

WAN Interface Setup

WAN Interface:: wan1_ppp

Zone: WAN

IP Address: 0.0.0.0

First DNS Server:

Second DNS Server:

The following table describes the labels in this screen.

Table 11 WAN and ISP Connection Settings

LABEL	DESCRIPTION
ISP Parameter	This section appears if the interface uses a PPPoE or PPTP Internet connection.
Encapsulation	This displays the type of Internet connection you are configuring.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ISG50 accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ISG50 accepts CHAP only. **PAP** - Your ISG50 accepts PAP only. **MSCHAP** - Your ISG50 accepts MSCHAP only. **MSCHAP-V2** - Your ISG50 accepts MSCHAP-V2 only.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.

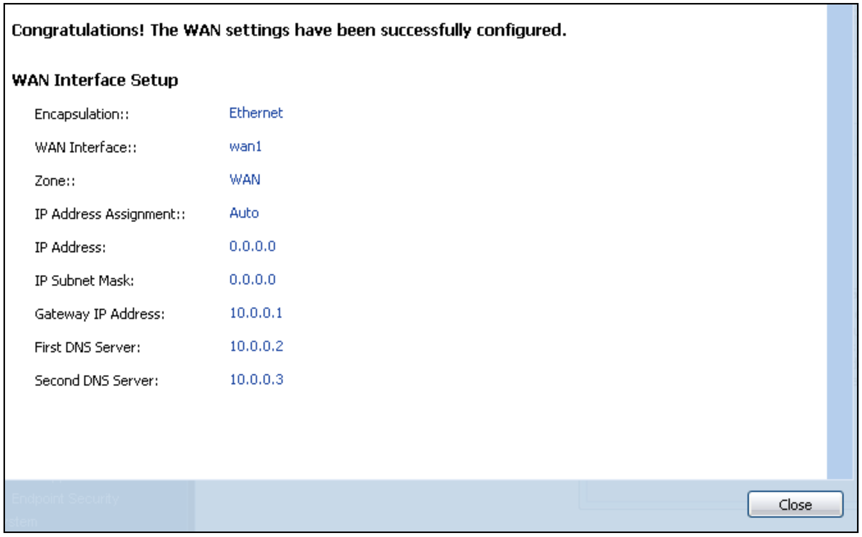
Table 11 WAN and ISP Connection Settings (continued)

LABEL	DESCRIPTION
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. 0 means no timeout.
PPTP Configuration	This section only appears if the interface uses a PPPoE or PPTP Internet connection.
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP	Type the IP address of the PPTP server.
Connection ID	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and **-_:** characters, and it can be up to 31 characters long.
WAN Interface Setup	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	This field is read-only when the WAN interface uses a dynamic IP address. If your WAN interface uses a static IP address, enter it in this field.
First DNS Server Second DNS Server	These fields only display for an interface with a static IP address. Enter the DNS server IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ISG50 uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

5.2.5 Quick Setup Interface Wizard: Summary

This screen displays the WAN interface's settings.

Figure 50 Interface Wizard: Summary WAN (PPTP Shown)



Congratulations! The WAN settings have been successfully configured.

WAN Interface Setup

Encapsulation::	Ethernet
WAN Interface::	wan1
Zone::	WAN
IP Address Assignment::	Auto
IP Address:	0.0.0.0
IP Subnet Mask:	0.0.0.0
Gateway IP Address:	10.0.0.1
First DNS Server:	10.0.0.2
Second DNS Server:	10.0.0.3

The following table describes the labels in this screen.

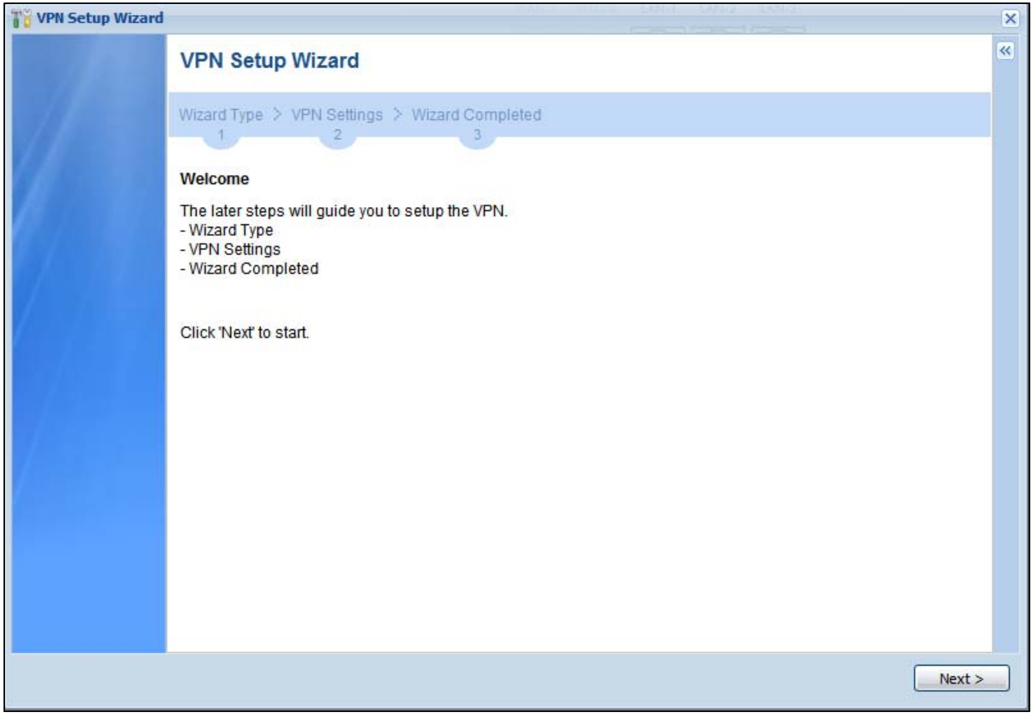
Table 12 Interface Wizard: Summary WAN

LABEL	DESCRIPTION
Encapsulation	This displays what encapsulation this interface uses to connect to the Internet.
Service Name	This field is read-only and only appears for a PPPoE interface. It displays the PPPoE service name specified in the ISP account.
Server IP	This field only appears for a PPTP interface. It displays the IP address of the PPTP server.
User Name	This is the user name given to you by your ISP.
Nailed-Up	If **No** displays the connection will not time out. **Yes** means the ISG50 uses the idle timeout.
Idle Timeout	This is how many seconds the connection can be idle before the router automatically disconnects from the PPPoE server. 0 means no timeout.
Connection ID	If you specified a connection ID, it displays here.
WAN Interface	This identifies the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address Assignment	This field displays whether the WAN IP address is static or dynamic (**Auto**).
First DNS Server Second DNS Server	If the **IP Address Assignment** is **Static**, these fields display the DNS server IP address(es).
Close	Click **Close** to exit the wizard.

5.3 VPN Quick Setup

Click **VPN Setup** in the main **Quick Setup** screen to open the **VPN Setup Wizard Welcome** screen. The VPN wizard creates corresponding VPN connection and VPN gateway settings and address objects that you can use later in configuring more VPN connections or other features. Click **Next**.

Figure 51 VPN Quick Setup Wizard


VPN Setup Wizard
VPN Setup Wizard
Wizard Type 1
VPN Settings 2
Wizard Completed 3
Next >

Welcome

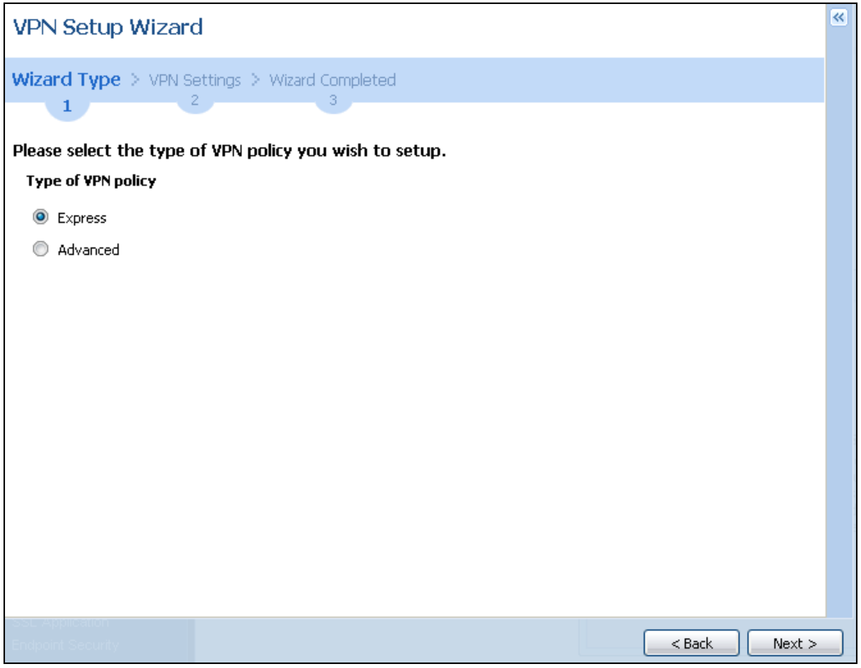
The later steps will guide you to setup the VPN.
- Wizard Type
- VPN Settings
- Wizard Completed

Click 'Next' to start.

5.4 VPN Setup Wizard: Wizard Type

A VPN (Virtual Private Network) tunnel is a secure connection to another computer, smartphone, or network. Use this screen to select which type of VPN connection you want to configure.

Figure 52 VPN Setup Wizard: Wizard Type



Please select the type of VPN policy you wish to setup.

Type of VPN policy

● Express

○ Advanced

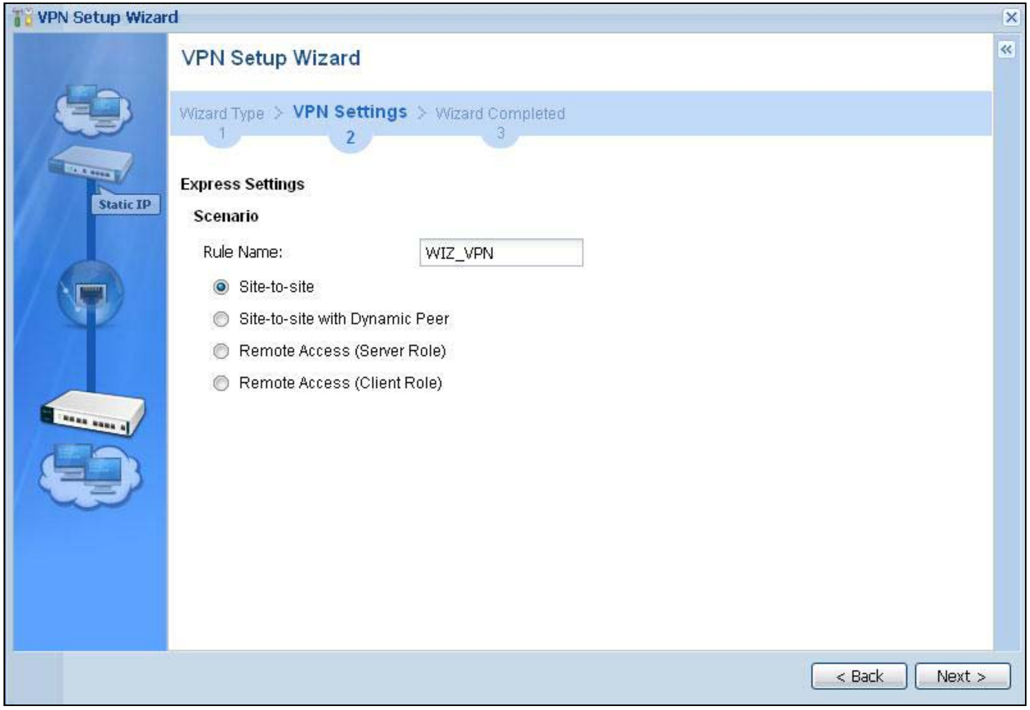
Express: Use this wizard to create a VPN connection with another ISG50 using a pre-shared key and default security settings.

Advanced: Use this wizard to configure detailed VPN security settings such as using certificates. The VPN connection can be to another ISG50 or other IPSec device.

5.5 VPN Express Wizard - Scenario

Click the **Express** radio button as shown in Figure 52 on page 77 to display the following screen.

Figure 53 VPN Express Wizard: Step 2



Express Settings

Scenario

Rule Name: WIZ_VPN

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

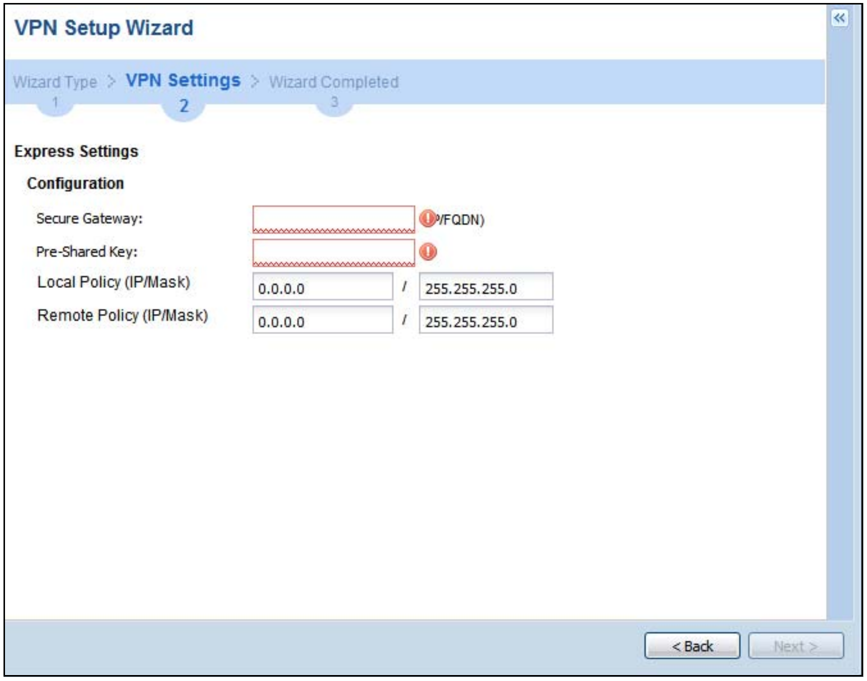
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- Site-to-site - Choose this if the remote IPSec device has a static IP address or a domain name. This ISG50 can initiate the VPN tunnel.
- Site-to-site with Dynamic Peer - Choose this if the remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- Remote Access (Server Role) - Choose this to allow incoming connections from IPSec VPN clients, including smartphone applications. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- Remote Access (Client Role) - Choose this to connect to an IPSec server. This ISG50 is the client (dial-in user) and can initiate the VPN tunnel.

See Application Scenarios on page 369 for more on the scenarios.

5.5.1 VPN Express Wizard - Configuration

Figure 54 VPN Express Wizard: Step 3



Express Settings

Configuration

Secure Gateway: (P/FQDN)

Pre-Shared Key:

Local Policy (IP/Mask) 0.0.0.0 / 255.255.255.0

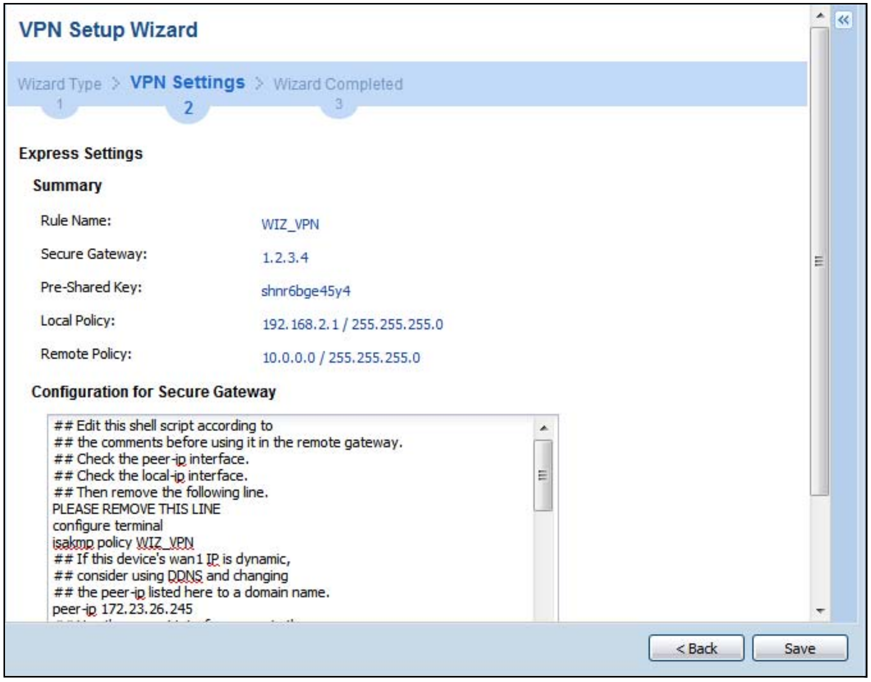
Remote Policy (IP/Mask) 0.0.0.0 / 255.255.255.0

- **Secure Gateway**: If **Any** displays in this field, it is not configurable for the chosen scenario. If this field is configurable, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec router by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address.
- **Pre-Shared Key**: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
- **Local Policy (IP/Mask)**: Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- **Remote Policy (IP/Mask)**: If **Any** displays in this field, it is not configurable for the chosen scenario. If this field is configurable, type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.

5.5.2 VPN Express Wizard - Summary

This screen provides a read-only summary of the VPN tunnel's configuration and also commands that you can copy and paste into another ISG50's command line interface to configure it.

Figure 55 VPN Express Wizard: Step 4



Express Settings

Summary

Rule Name: WIZ_VPN
Secure Gateway: 1.2.3.4
Pre-Shared Key: shnr6bge45y4
Local Policy: 192.168.2.1 / 255.255.255.0
Remote Policy: 10.0.0.0 / 255.255.255.0

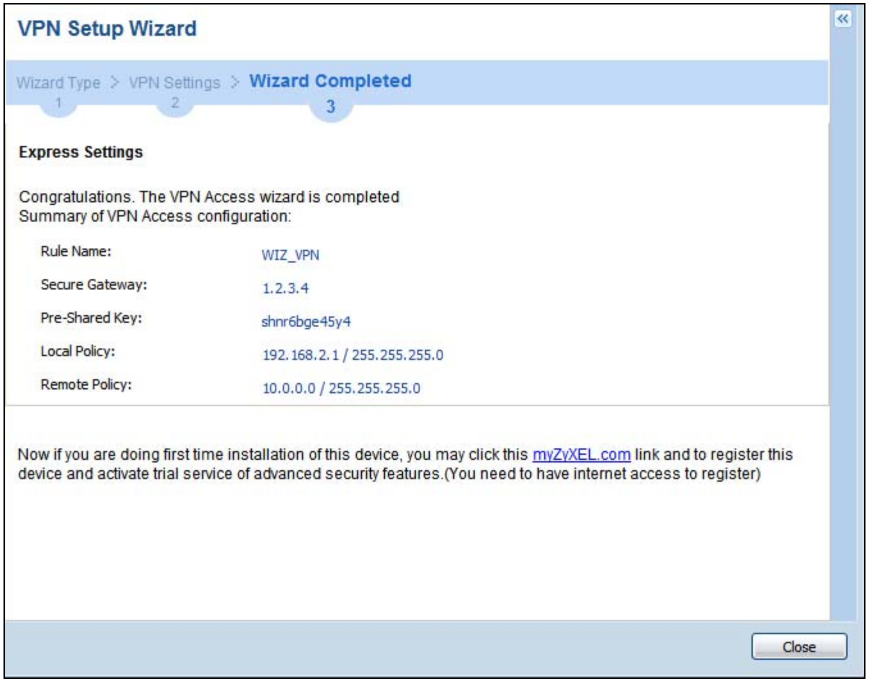
Configuration for Secure Gateway

```
## Edit this shell script according to
## the comments before using it in the remote gateway.
## Check the peer-ip interface.
## Check the local-ip interface.
## Then remove the following line.
PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN
## If this device's wan1 IP is dynamic,
## consider using DDNS and changing
## the peer-ip listed here to a domain name.
peer-ip 172.23.26.245
```

- **Rule Name**: Identifies the VPN gateway policy.
- **Secure Gateway**: IP address or domain name of the remote IPSec device. If this field displays **Any**, only the remote IPSec device can initiate the VPN connection.
- **Pre-Shared Key**: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy**: (Static) IP address and subnet mask of the computers on the network behind your ISG50 that can use the tunnel.
- **Remote Policy**: (Static) IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel. If this field displays **Any**, only the remote IPSec device can initiate the VPN connection.
- Copy and paste the **Configuration for Secure Gateway** commands into another ISG50's command line interface to configure it to serve as the other end of this VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.

5.5.3 VPN Express Wizard - Finish

Now you can use the VPN tunnel.



Express Settings

Congratulations. The VPN Access wizard is completed
Summary of VPN Access configuration:

Rule Name:	WIZ_VPN
Secure Gateway:	1.2.3.4
Pre-Shared Key:	shnr6bge45y4
Local Policy:	192.168.2.1 / 255.255.255.0
Remote Policy:	10.0.0.0 / 255.255.255.0

Now if you are doing first time installation of this device, you may click this myZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)

Figure 56 VPN Express Wizard: Finish

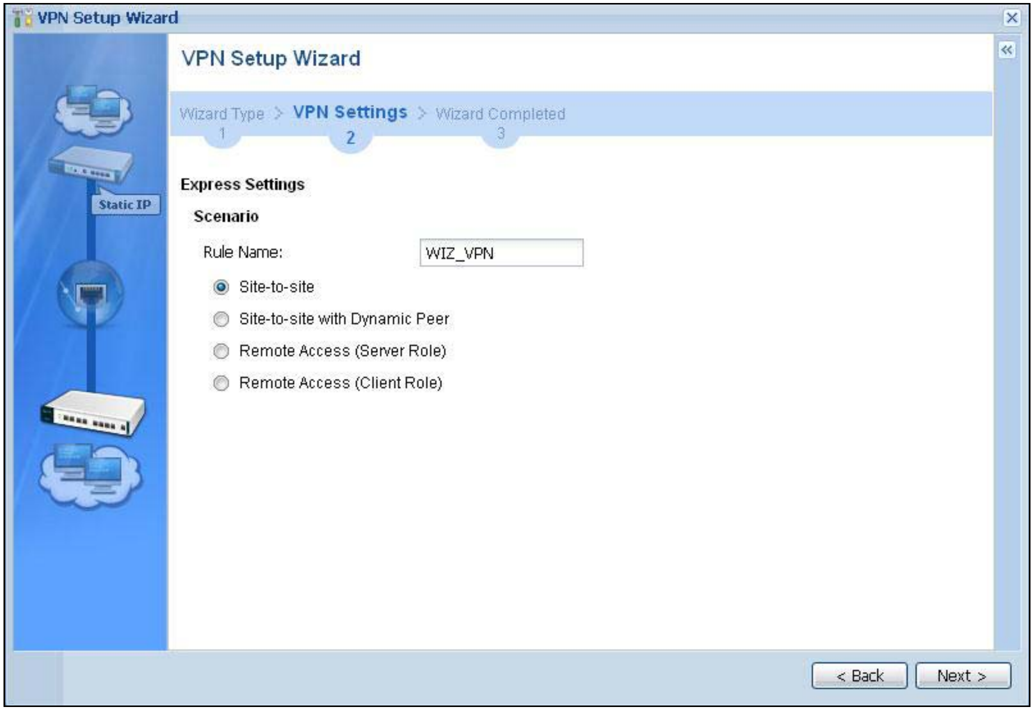
Note: If you have not already done so, use the myZyXEL.com link and register your ISG50 with myZyXEL.com.

Click **Close** to exit the wizard.

5.5.4 VPN Advanced Wizard - Scenario

Click the **Advanced** radio button as shown in Figure 52 on page 77 to display the following screen.

Figure 57 VPN Advanced Wizard: Scenario



Express Settings

Scenario

Rule Name: WIZ_VPN

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

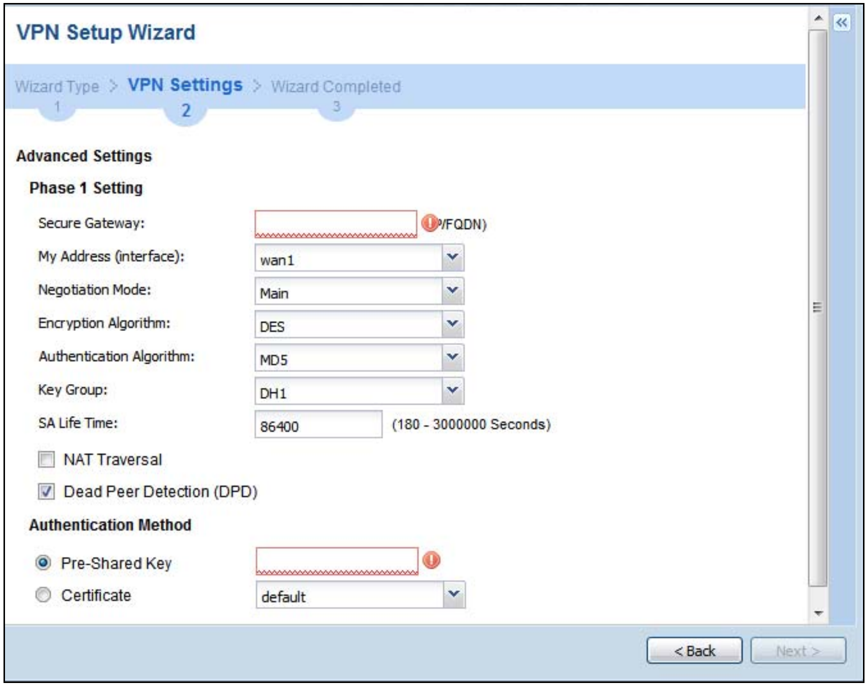
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- Site-to-site - Choose this if the remote IPSec device has a static IP address or a domain name. This ISG50 can initiate the VPN tunnel.
- Site-to-site with Dynamic Peer - Choose this if the remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- Remote Access (Server Role) - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- Remote Access (Client Role) - Choose this to connect to an IPSec server. This ISG50 is the client (dial-in user) and can initiate the VPN tunnel.

5.5.5 VPN Advanced Wizard - Phase 1 Settings

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Figure 58 VPN Advanced Wizard: Phase 1 Settings



Advanced Settings

Phase 1 Setting

Secure Gateway: P/FQDN)
My Address (interface): wan1
Negotiation Mode: Main
Encryption Algorithm: DES
Authentication Algorithm: MD5
Key Group: DH1
SA Life Time: 86400 (180 - 3000000 Seconds)
☐ NAT Traversal
☑ Dead Peer Detection (DPD)

Authentication Method

● Pre-Shared Key
○ Certificate default

- **Secure Gateway**: If **Any** displays in this field, it is not configurable for the chosen scenario. If this field is configurable, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec device by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec device has a dynamic WAN IP address.
- **My Address (interface)**: Select an interface from the drop-down list box to use on your ISG50.
- **Negotiation Mode**: Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Note: Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. AES128 uses a 128-bit key and is faster than 3DES. AES192 uses a 192-bit key and AES256 uses a 256-bit key.
- **Authentication Algorithm**: **MD5** gives minimal security. **SHA-1** gives higher security. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower.
- **Key Group**: **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number.

- **SA Life Time**: Set how often the ISG50 renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **NAT Traversal**: Select this if the VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices).

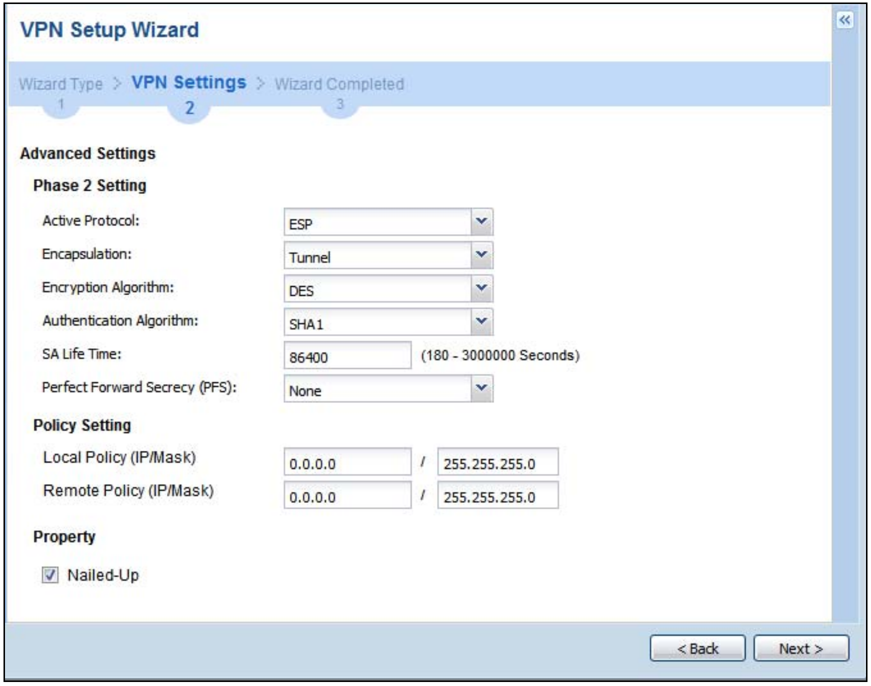
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens or the User's Guide VPN, NAT, and NAT Traversal on page 390 for more information.

- **Dead Peer Detection (DPD)** has the ISG50 make sure the remote IPSec device is there before transmitting data through the IKE SA. If there has been no traffic for at least 15 seconds, the ISG50 sends a message to the remote IPSec device. If it responds, the ISG50 transmits the data. If it does not respond, the ISG50 shuts down the IKE SA.
- **Authentication Method**: Select **Pre-Shared Key** to use a password or **Certificate** to use one of the ISG50's certificates.

5.5.6 VPN Advanced Wizard - Phase 2

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPSec.

Figure 59 VPN Advanced Wizard: Step 4



Advanced Settings

Phase 2 Setting

Active Protocol: ESP

Encapsulation: Tunnel

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time: 86400 (180 - 3000000 Seconds)

Perfect Forward Secrecy (PFS): None

Policy Setting

Local Policy (IP/Mask) 0.0.0.0 / 255.255.255.0

Remote Policy (IP/Mask) 0.0.0.0 / 255.255.255.0

Property

☑ Nailed-Up

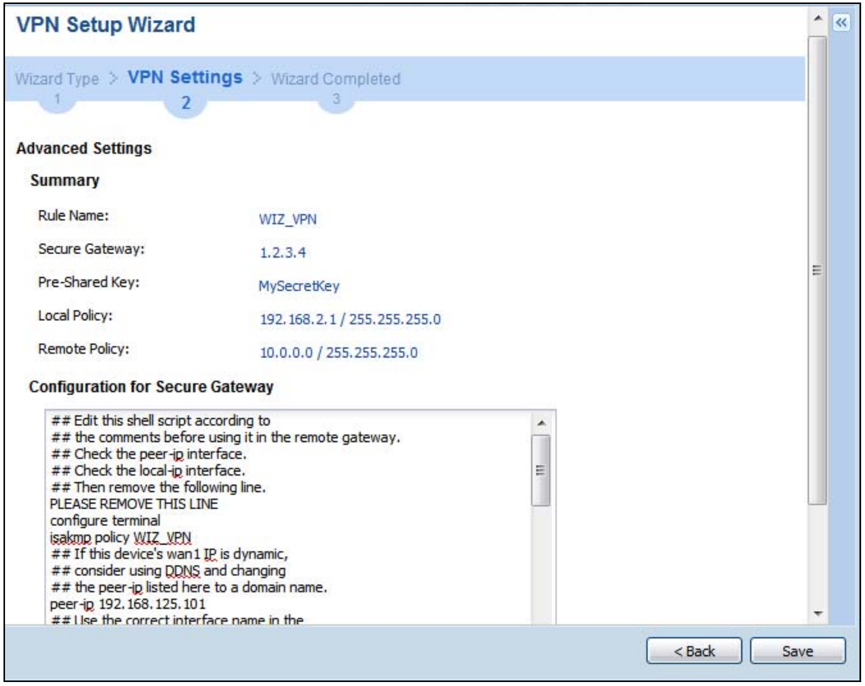
- **Active Protocol**: **ESP** is compatible with NAT, **AH** is not.
- **Encapsulation**: **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.
- **Authentication Algorithm**: **MD5** gives minimal security. **SHA-1** gives higher security. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower.
- **SA Life Time**: Set how often the ISG50 renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.

- Perfect Forward Secrecy (PFS): Disabling PFS allows faster IPSec setup, but is less secure. Select DH1, DH2 or DH5 to enable PFS. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
- **Local Policy (IP/Mask)**: Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- **Remote Policy (IP/Mask)**: Type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.
- **Nailed-Up**: This displays for the site-to-site and remote access client role scenarios. Select this to have the ISG50 automatically renegotiate the IPSec SA when the SA life time expires.

5.5.7 VPN Advanced Wizard - Summary

This is a read-only summary of the VPN tunnel settings.

Figure 60 VPN Advanced Wizard: Step 5



Advanced Settings

Summary

Rule Name: WIZ_VPN
Secure Gateway: 1.2.3.4
Pre-Shared Key: MySecretKey
Local Policy: 192.168.2.1 / 255.255.255.0
Remote Policy: 10.0.0.0 / 255.255.255.0

Configuration for Secure Gateway

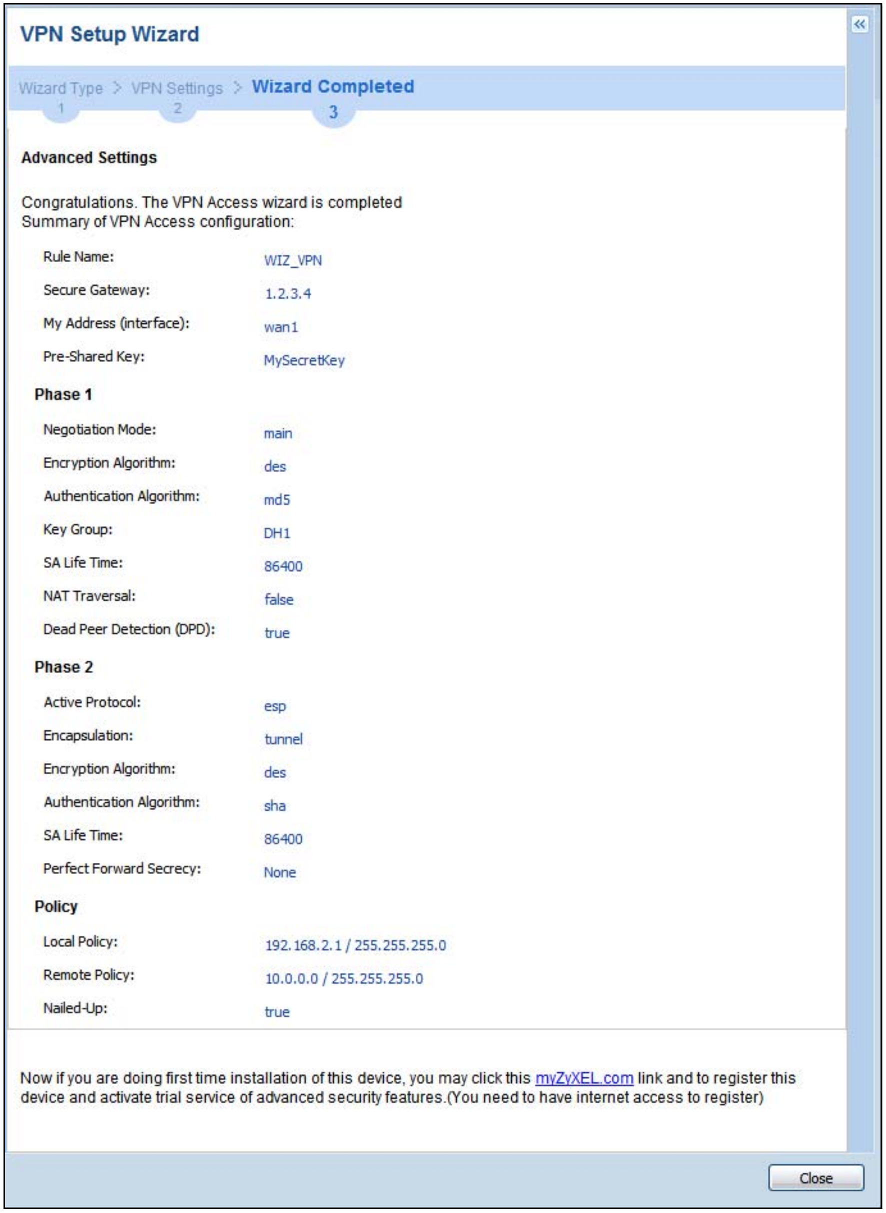
```
## Edit this shell script according to
## the comments before using it in the remote gateway.
## Check the peer-ip interface.
## Check the local-ip interface.
## Then remove the following line.
PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN
## If this device's wan1 IP is dynamic,
## consider using DDNS and changing
## the peer-ip listed here to a domain name.
peer-ip 192.168.125.101
## Use the correct interface name in the
```

- **Rule Name**: Identifies the VPN connection (and the VPN gateway).
- **Secure Gateway**: IP address or domain name of the remote IPSec device.
- **Pre-Shared Key**: VPN tunnel password.
- **Certificate**: The certificate the ISG50 uses to identify itself when setting up the VPN tunnel.
- **Local Policy**: IP address and subnet mask of the computers on the network behind your ISG50 that can use the tunnel.
- **Remote Policy**: IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel.
- Copy and paste the **Configuration for Remote Gateway** commands into another ISG50's command line interface.
- Click **Save** to save the VPN rule.

5.5.8 VPN Advanced Wizard - Finish

Now you can use the VPN tunnel.

Figure 61 VPN Wizard: Step 6: Advanced



Advanced Settings

Congratulations. The VPN Access wizard is completed
Summary of VPN Access configuration:

Rule Name: WIZ_VPN
Secure Gateway: 1.2.3.4
My Address (interface): wan1
Pre-Shared Key: MySecretKey

Phase 1

Negotiation Mode: main
Encryption Algorithm: des
Authentication Algorithm: md5
Key Group: DH1
SA Life Time: 86400
NAT Traversal: false
Dead Peer Detection (DPD): true

Phase 2

Active Protocol: esp
Encapsulation: tunnel
Encryption Algorithm: des
Authentication Algorithm: sha
SA Life Time: 86400
Perfect Forward Secrecy: None

Policy

Local Policy: 192.168.2.1 / 255.255.255.0
Remote Policy: 10.0.0.0 / 255.255.255.0
Nailed-Up: true

Now if you are doing first time installation of this device, you may click this myZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)

Note: If you have not already done so, you can register your ISG50 with myZyXEL.com and activate trials of services.

Click **Close** to exit the wizard.

6

Configuration Basics

This information is provided to help you configure the ISG50 effectively. Some of it is helpful when you are just getting started. Some of it is provided for your reference when you configure various features in the ISG50.

- Section 6.2 on page 91 introduces the ISG50's object-based configuration.
- Section 6.3 on page 92 introduces zones, interfaces, and port groups.
- Section 6.4 on page 94 introduces some terminology and organization for the ISG50.
- Section 6.5 on page 94 covers the ISG50's packet flow.
- Section 6.6 on page 97 identifies the features you should configure before and after you configure the main screens for each feature. For example, if you want to configure a trunk for load-balancing, you should configure the member interfaces before you configure the trunk. After you configure the trunk, you should configure a policy route for it as well. (You might also have to configure criteria for the policy route.)
- Section 6.7 on page 103 identifies the objects that store information used by other features.
- Section 6.8 on page 104 introduces some of the tools available for system management.

6.1 PBX Features Overview

This chapter is an overview of different logical components and how they work together to route calls on the ISG50.

6.1.1 Call Routing

The two main functions of any IP-PBX are routing internal calls and handling calls to and from the outside world.

The following sections explain how these functions are performed on the ISG50.

6.1.1.1 Call Routing Terms

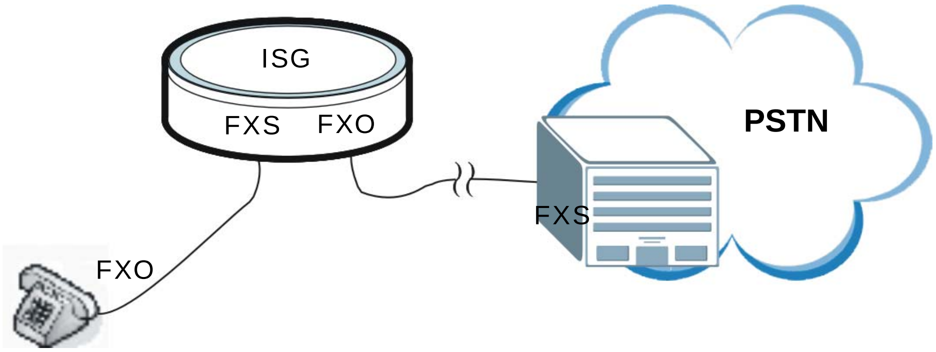
The following are some terms related to ZyXEL's IP-PBX implementation.

- **Extension** - This is a unique number assigned to each telephone connected to the ISG50. Extensions are used to make calls between phones connected to the ISG50 and to route calls from the outside world to their correct target. Extensions fall into the following two groups:
  - **SIP Extension** - This is an extension assigned to a SIP (Session Initiation Protocol) based IP phone connected to the ISG50. Alternatively this could be an extension assigned to an analog phone which connects to the ISG50 via a VoIP gateway device.

  - FXS (Foreign Exchange Subscriber) Extension - This is an extension assigned to an analog phone directly connected to an FXS port on the ISG50 (See Figure 62 on page 88). The FXS ports on the ISG50 work the same way as the phone sockets in your home. In your home you are a subscriber to the telephone services of your local telephone company and when you connect an analog phone to the ISG50 you subscribe to the telephone services of the ISG50.
- **Authority Group** - This is a set of extensions. Each extension can only belong to one authority group. Authority groups manage extensions by allowing them to make only certain types of calls. For example, if you create two authority groups, you can allow one group to make local calls and long distance calls and the second authority group to make local calls only.
- **Outbound Line Group** - This is a set of connections or lines going to the outside world.
  - **SIP Trunk** - This is a connection to your ITSP (Internet Telephony Service Provider).
  - **ISDN BRI Trunk** - This is a connection to your ISDN Service Provider.
  - **Trusted Peer** - This is a connection to another IP PBX or SIP server. The trusted peer device must also specify your ISG50 as a trusted peer.
  - **FXO (Foreign Exchange Office) Trunk** - This type of outbound line group consists of telephone cables connected to FXO ports on the ISG50. The telephone cables lead to the PSTN (Public Switched Telephone Network), or in other words your traditional (non-VoIP) telephone company. FXO ports always point in the direction of the telephone services.

  The figure below shows the relationship between FXS and FXO ports.

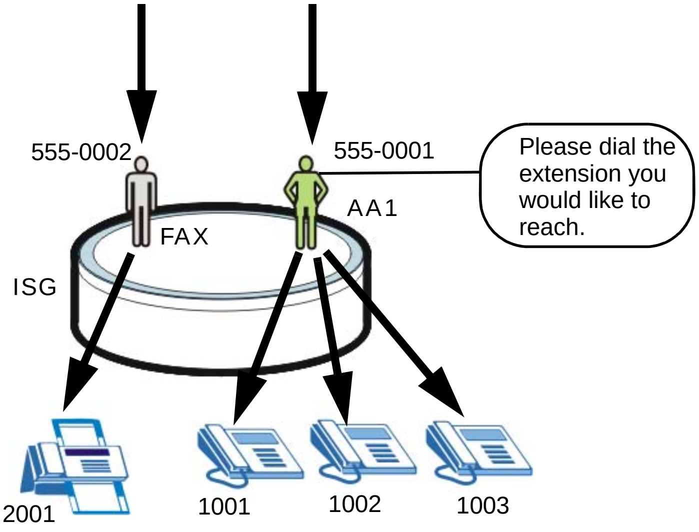
Figure 62 FXS and FXO Ports



- **LCR (Least Cost Routing)** - This is a rule which specifies which outbound line group is used when making an outbound call. It consists of a dialing condition, for example dial **0** to make a call via a specific FXO trunk or dial **1** for calls via a SIP trunk. LCRs also set priority to which outbound line group should be tried first, second, third and so on when making outbound calls with the same dialing condition.

- **Auto-Attendant** - This is a feature which routes incoming calls to their proper extension. An auto-attendant is assigned to each outbound line group and it services incoming calls on those lines. If your organization has two outbound line groups, each with a specific telephone number for incoming calls, then you can assign a different auto-attendant for each incoming line. Assign one auto-attendant for general calls to the extensions in your organization (for example **AA1**) and one auto-attendant for direct routing to a FAX machine (for example **FAX**).

Figure 63 Auto-Attendant



6.1.2 Internal Call Routing

Internal call routing refers to calls between extensions on the ISG50. People simply dial the extension they want to call. The ISG50 checks to see if the number dialed is an existing extension and forwards the call to that extension. The ISG50 by default allows people with extensions from one authority group to call extensions in another authority group. You can, however, block calls between authority groups if your organization requires such a setting.

The configuration requirement for setting up internal call routing are:

1 Create an authority group.

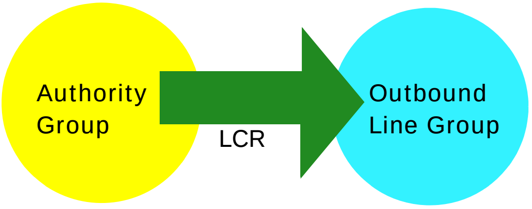
2 Create extensions in the authority group.

6.1.3 Outbound Call Routing

Outbound call routing refers to calls originating from an extension on the ISG50, going via an outbound line group to a telephone outside your organization. Outbound call routing requires that an authority group is linked to an outbound line group. The link between the two is an LCR (Least Cost Routing). LCRs contain the dialing rules for outbound line groups. Authority groups need to be associated to LCRs to gain access to the outbound line groups.

In the most basic setup example an organization has one authority group (with all of the company's extensions), one outbound line group and an LCR which grants the authority group access to outbound lines. Everyone in the organization has the same rights to use outbound lines.

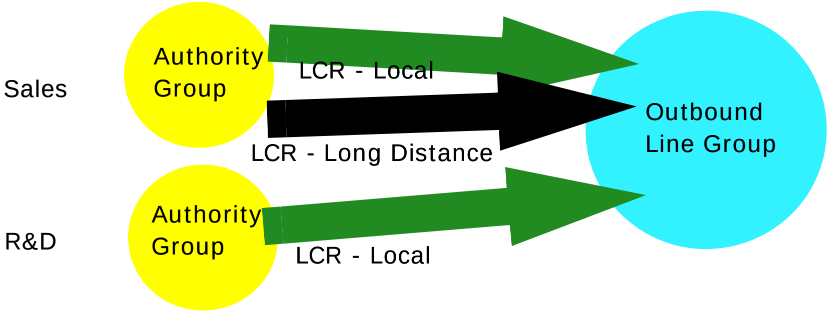
Figure 64 Outbound Call Routing - Basic


Authority Group
LCR
Outbound Line Group

In a more advanced example, you can create two authority groups, still have one outbound line group and two different LCRs. You can now control the types of outbound calls that can be made by each authority group.

In the figure below, the **SALES** authority group has a local call LCR and a long distance LCR associated to it. This allows its group members to make both local and long distance calls via the outbound line group. R&D authority group only has the local LCR associated to it so its group members can only make local calls via the outbound line group.

Figure 65 Outbound Call Routing - Advanced


Sales
Authority Group
LCR - Local
LCR - Long Distance
Outbound Line Group
R&D
Authority Group
LCR - Local

The configuration requirement for setting up outbound call routing are:

1. Create an authority group.
2. Create extensions in the authority group.
3. Create an outbound line group.
4. Create LCRs and add outbound line groups to them.
5. Associate LCRs to authority groups.

6.2 Object-based Configuration

The ISG50 stores information or settings as objects. You use these objects to configure many of the ISG50’s features and settings. Once you configure an object, you can reuse it in configuring other features.

When you change an object’s settings, the ISG50 automatically updates all the settings or rules that use the object. For example, if you create a schedule object, you can have firewall and other settings use it. If you modify the schedule, all the firewall and other settings that use the schedule automatically apply the updated schedule.

You can create address objects based on an interface’s IP address, subnet, or gateway. The ISG50 automatically updates every rule or setting that uses these objects whenever the interface’s IP address settings change. For example, if you change an Ethernet interface’s IP address, the ISG50 automatically updates the rules or settings that use the interface-based, LAN subnet address object.

You can use the **Configuration > Objects** screens to create objects before you configure features that use them. If you are in a screen that uses objects, you can also usually select **Create new Object** to be able to configure a new object. For a list of common objects, see Section 6.7 on page 103.

Use the **Object Reference** screen (Section 3.3.3.3 on page 53) to see what objects are configured and which configuration settings reference specific objects.

6.3 Zones, Interfaces, and Physical Ports

Zones (groups of interfaces and VPN tunnels) simplify security settings. Here is an overview of zones, interfaces, and physical ports in the ISG50.

Figure 66 Zones, Interfaces, and Physical Ethernet Ports

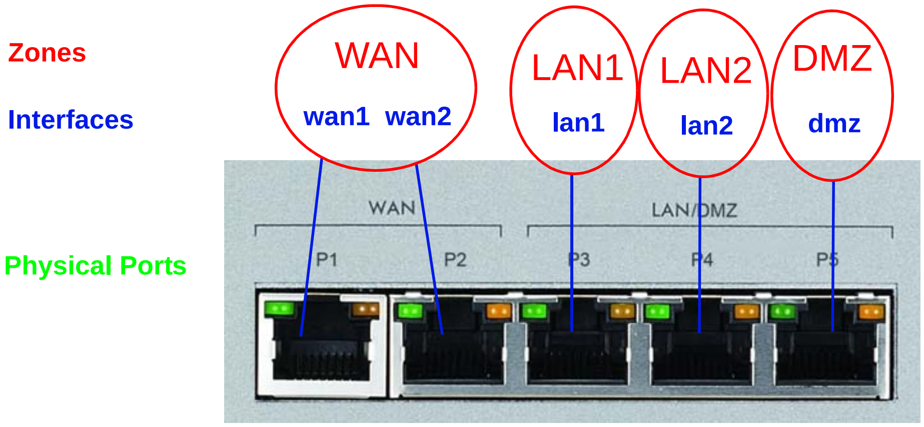


Table 13 Zones, Interfaces, and Physical Ethernet Ports

Zones (WAN,LAN, DMZ)	A zone is a group of interfaces and VPN tunnels. Use zones to apply security settings such as firewall, and remote management.
Interfaces (Ethernet, VLAN,...)	Interfaces are logical entities that (layer-3) packets pass through. Use interfaces in configuring VPN, zones, trunks, DDNS, policy routes, static routes, HTTP redirect, and NAT. Port roles combine physical ports into interfaces.
Physical Ethernet Ports (P1, P2, ...)	The physical port is where you connect a cable. In configuration, you use physical ports when configuring port groups. You use interfaces and zones in configuring other features.

6.3.1 Interface Types

There are many types of interfaces in the ISG50. In addition to being used in various features, interfaces also describe the network that is directly connected to the ISG50.

- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. You also configure RIP and OSPF in these interfaces.
- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level. Port groups are created when you use the **Interface > Port Roles** screen to set multiple physical ports to be part of the same (lan1, lan2 or dmz) interface.
- **PPP interfaces** support Point-to-Point Protocols (PPPoE or PPTP). ISP accounts are required for PPPoE/PPTP interfaces.
- **VLAN interfaces** recognize tagged frames. The ISG50 automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Then, you can configure the IP address and subnet mask of the bridge. It is also possible to configure zone-level security between the member interfaces in the bridge.

- **Virtual interfaces** increase the amount of routing information in the ISG50. There are three types: **virtual Ethernet interfaces** (also known as IP alias), **virtual VLAN interfaces**, and **virtual bridge interfaces**.

6.3.2 Default Interface and Zone Configuration

This section introduces the ISG50's default zone member physical interfaces and the default configuration of those interfaces. The following figure uses letters to denote public IP addresses or part of a private IP address.

Figure 67 Default Network Topology

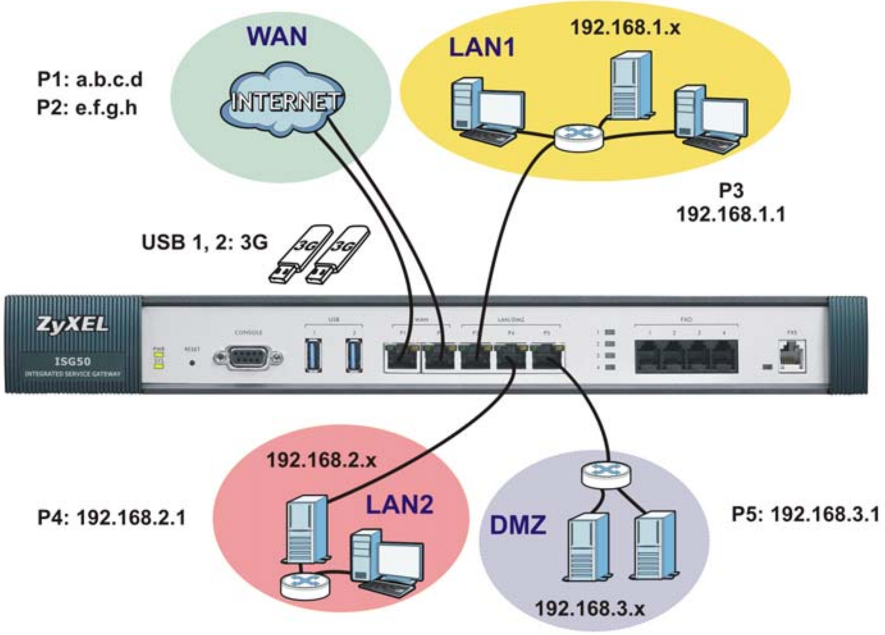


Table 14 ISG50 Default Port, Interface, and Zone Configuration

PORT	INTERFACE	ZONE	IP ADDRESS AND DHCP SETTINGS	SUGGESTED USE WITH DEFAULT SETTINGS
P1, P2	wan1, wan2	WAN	DHCP clients	Connections to the Internet
P3	lan1	LAN1	192.168.1.1, DHCP server enabled	Protected LAN
P4	lan2	LAN2	192.168.2.1, DHCP server enabled	Protected LAN
P5	dmz	DMZ	192.168.3.1, DHCP server disabled	Public servers (such as web, e-mail and FTP)
CONSOLE	n/a	None	None	Local management

- The WAN zone contains the **wan1** and **wan2** interfaces (physical ports **P1** and **P2**). They use public IP addresses to connect to the Internet.
- The LAN1 zone contains the **lan1** interface (physical port **P3**). The LAN1 zone is a protected zone. The **lan1** interface uses 192.168.1.1 and the connected devices use IP addresses in the 192.168.1.2 to 192.168.1.254 range.
- The LAN2 zone contains the **lan2** interface (physical port **P4**). The LAN2 zone is a protected zone. The **lan2** interface uses 192.168.2.1 and the connected devices use IP addresses in the 192.168.2.2 to 192.168.2.254 range.
- The DMZ zone contains the **dmz** interface (physical port **P5**). The DMZ zone has servers that are available to the public. The **dmz** interface uses private IP address 192.168.3.1 and the connected devices use private IP addresses in the 192.168.3.2 to 192.168.3.254 range.

6.4 Terminology in the ISG50

This section highlights some terminology or organization for the ISG50.

Table 15 ISG50 Terminology

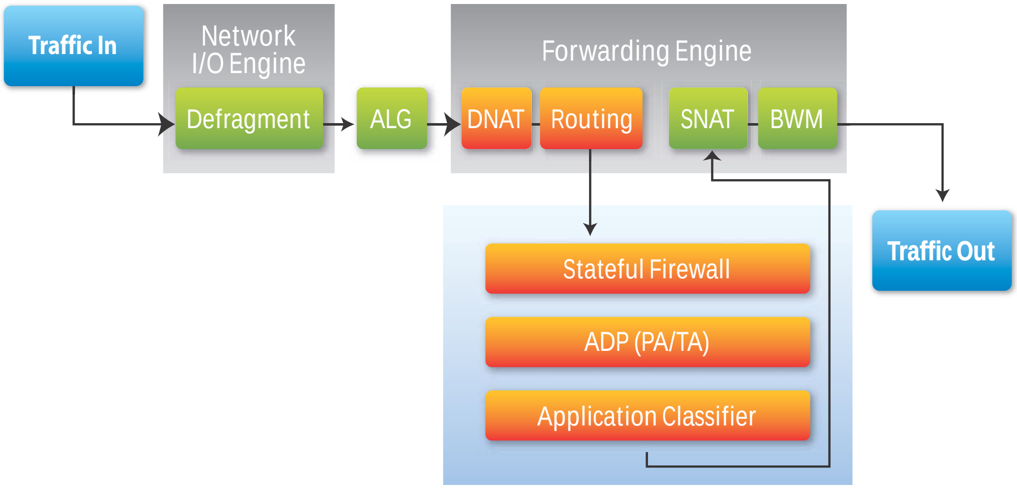
FEATURE / TERM	ISG50 FEATURE / TERM
IP alias	Virtual interface
Gateway policy	VPN gateway
Network policy (IPSec SA)	VPN connection
Source NAT (SNAT)	Policy route
Trigger port, port triggering	Policy route
Address mapping	Policy route
Address mapping (VPN)	IPSec VPN
Interface bandwidth management (outbound)	Interface
General bandwidth management	Policy route

6.5 Packet Flow

Here is the order in which the ISG50 applies its features and checks.

Traffic in > Defragmentation > Destination NAT > Routing > Stateful Firewall > ADP > SNAT > Bandwidth Management > Fragmentation > Traffic Out.

Figure 68 Packet Flow


Traffic In
Network I/O Engine
Defragment
ALG
Forwarding Engine
DNAT
Routing
SNAT
BWM
Stateful Firewall
ADP (PA/TA)
Application Classifier
Traffic Out

The packet flow is as follows:

- Automatic SNAT and WAN trunk routing for traffic going from internal to external interfaces (you don't need to configure anything to all LAN to WAN traffic).

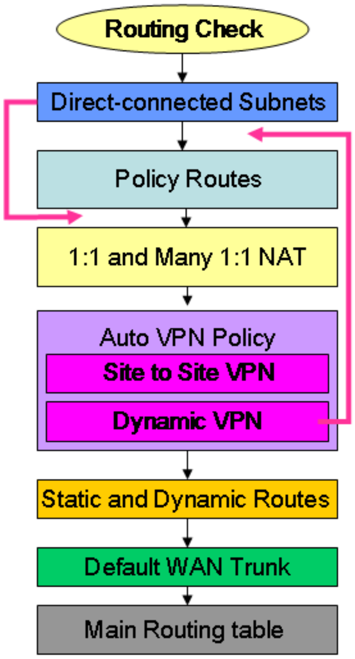
  The ISG50 automatically adds all of the external interfaces to the default WAN trunk. External interfaces include ppp and cellular interfaces as well as any Ethernet interfaces that are set as external interfaces.

  Examples of internal interfaces are any Ethernet interfaces that you configure as internal interfaces.
- A policy route can be automatically disabled if the next-hop is dead.
- You do not need to set up policy routes for IPSec traffic.
- Policy routes can override direct routes.
- You do not need to set up policy routes for 1:1 NAT entries.
- You can create Many 1:1 NAT entries to translate a range of private network addresses to a range of public IP addresses
- Static and dynamic routes have their own category.

6.5.1 Routing Table Checking Flow

When the ISG50 receives packets it defragments them and applies destination NAT. Then it examines the packets and determines how to route them. The checking flow is from top to bottom. As soon as the packets match an entry in one of the sections, the ISG50 stops checking the packets against the routing table and moves on to the other checks, for example the firewall check.

Figure 69 Routing Table Checking Flow



1 **Direct-connected Subnets**: The ISG50 first checks to see if the packets are destined for an address in the same subnet as one of the ISG50's interfaces. You can override this and have the ISG50 check the policy routes first by enabling the policy route feature's **Use Policy Route to Override Direct Route** option (see Section 14.1 on page 289).

2. **Policy Routes**: These are the user-configured policy routes. Configure policy routes to send packets through the appropriate interface or VPN tunnel. See Chapter 14 on page 289 for more on policy routes.

3. **1 to 1 and Many 1 to 1 NAT**: These are the 1 to 1 NAT and many 1 to 1 NAT rules. If a private network server will initiate sessions to the outside clients, create a 1 to 1 NAT entry to have the ISG50 translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server. A many 1 to 1 NAT entry works like multiple 1 to 1 NAT rules. It maps a range of private network servers that will initiate sessions to the outside clients to a range of public IP addresses. See Section 18.2.1 on page 325 for more.

4. **Auto VPN Policy**: The ISG50 automatically creates these routing entries for the VPN rules. Disabling the IPSec VPN feature's **Use Policy Route to control dynamic IPSec rules** option moves the routes for dynamic IPSec rules up above the policy routes (see Section 24.2 on page 370).

5. **Static and Dynamic Routes**: This section contains the user-configured static routes and the dynamic routing information learned from other routers through RIP and OSPF. See Chapter 14 on page 289 for more information.

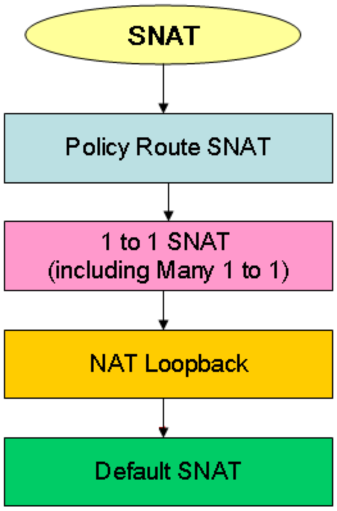
6. **Default WAN Trunk**: For any traffic coming in through an internal interface, if it does not match any of the other routing entries, the ISG50 forwards it through the default WAN trunk. See Section 13.2 on page 285 for how to select which trunk the ISG50 uses as the default.

7. **Main Routing Table**: The default WAN trunk is expected to be used for any traffic that did not match any earlier routing entries.

6.5.2 NAT Table Checking Flow

The checking flow is from top to bottom. As soon as the packets match an entry in one of the sections, the ISG50 stops checking the packets against the NAT table and moves on to bandwidth management.

Figure 70 NAT Table Checking Flow



1. SNAT defined in the policy routes.
2. 1 to 1 SNAT (including Many 1 to 1) is also included in the NAT table.
3. NAT loopback is now included in the NAT table instead of requiring a separate policy route.
4. SNAT is also now performed by default and included in the NAT table.

6.6 Other Features Configuration Overview

This section provides information about configuring the main features in the ISG50. The features are listed in the same sequence as the menu item(s) in the Web Configurator. Each feature description is organized as shown below.

6.6.1 Feature

This provides a brief description. See the appropriate chapter(s) in this User's Guide for more information about any feature.

MENU ITEM(S)	This shows you the sequence of menu items and tabs you should click to find the main screen(s) for this feature. See the web help or the related User's Guide chapter for information about each screen.
PREREQUISITES	These are other features you should configure before you configure the main screen(s) for this feature. If you did not configure one of the prerequisites first, you can often select an option to create a new object. After you create the object you return to the main screen to finish configuring the feature. You may not have to configure everything in the list of prerequisites. For example, you do not have to create a schedule for a policy route unless time is one of the criterion.
WHERE USED	There are two uses for this. These are other features you should usually configure or check right after you configure the main screen(s) for this feature. For example, you should usually create a policy route for a VPN tunnel. You have to delete the references to this feature before you can delete any settings. For example, you have to delete (or modify) all the policy routes that refer to a VPN tunnel before you can delete the VPN tunnel.

Example: This provides a simple example to show you how to configure this feature. The example is usually based on the network topology in Figure 67 on page 93.

Note: **PREQUISITES** or **WHERE USED** does not appear if there are no prerequisites or references in other features to this one. For example, no other features reference DDNS entries, so there is no **WHERE USED** entry.

6.6.2 Licensing Registration

Use these screens to register your ISG50 and subscribe to services. You must have Internet access to myZyXEL.com.

MENU ITEM(S)	**Configuration > Licensing > Registration**
PREREQUISITES	Internet access to myZyXEL.com

6.6.3 Interface

See Section 6.3 on page 92 for background information.

Note: When you create an interface, there is no security applied on it until you assign it to a zone.

Most of the features that use interfaces support Ethernet, PPPoE/PPTP, cellular, VLAN, and bridge interfaces.

MENU ITEM(S)	**Configuration > Network > Interface** (except **Network > Interface > Trunk**)
PREREQUISITES	Port groups (configured in the **Interface > Port Grouping** screen)
WHERE USED	Zones, trunks, IPSec VPN, DDNS, policy routes, static routes, HTTP redirect, NAT

Example: The **dmz** interface is in the DMZ zone and uses a private IP address. To configure **dmz**'s settings, click **Network > Interface > Ethernet** and then the **dmz**'s **Edit** icon.

6.6.4 Trunks

Use trunks to set up load balancing using two or more interfaces.

MENU ITEM(S)	**Configuration > Network > Interface > Trunk**
PREREQUISITES	Interfaces
WHERE USED	Policy routes

Example: See Chapter 7 on page 107.

6.6.5 Policy Routes

Use policy routes to override the ISG50's default routing behavior in order to send packets through the appropriate interface or VPN tunnel. You can also use policy routes for bandwidth management (out of the ISG50), port triggering, and general NAT on the source address. You have to set up the criteria, next-hops, and NAT settings first.

MENU ITEM(S)	**Configuration > Network > Routing > Policy Route**

PREREQUISITES	Criteria: users, user groups, interfaces (incoming), IPSec VPN (incoming), addresses (source, destination), address groups (source, destination), schedules, services, service groups Next-hop: addresses (HOST gateway), IPSec VPN, trunks, interfaces NAT: addresses (translated address), services and service groups (port triggering)

Example: You have an FTP server connected to **P6** (in the DMZ zone). You want to limit the amount of FTP traffic that goes out from the FTP server through your WAN connection.

1. Create an address object for the FTP server (**Object > Address**).
2. Click **Configuration > Network > Routing > Policy Route** to go to the policy route configuration screen. Add a policy route.
3. Name the policy route.
4. Select the interface that the traffic comes in through (**P3** in this example).
5. Select the FTP server's address as the source address.
6. You don't need to specify the destination address or the schedule.
7. For the service, select **FTP**.
8. For the **Next Hop** fields, select **Interface** as the **Type** if you have a single WAN connection or **Trunk** if you have multiple WAN connections.
9. Select the interface that you are using for your WAN connection (**wan1** and **wan2** are the default WAN interfaces). If you have multiple WAN connections, select the trunk.
10. Specify the amount of bandwidth FTP traffic can use. You may also want to set a low priority for FTP traffic.

Note: The ISG50 checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that would also match the FTP traffic.

6.6.6 Static Routes

Use static routes to tell the ISG50 about networks not directly connected to the ISG50.

MENU ITEM(S)	**Configuration > Network > Routing > Static Route**
PREREQUISITES	Interfaces

6.6.7 Zones

See Section 6.3 on page 92 for background information. A zone is a group of interfaces and VPN tunnels. The ISG50 uses zones, not interfaces, in many security settings, such as firewall rules and remote management.

Zones cannot overlap. Each interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run. When you create a zone, the ISG50 does not create any firewall rule or configure remote management for the new zone.

MENU ITEM(S)	**Configuration > Network > Zone**
PREREQUISITES	Interfaces, IPSec VPN
WHERE USED	Firewall, remote management, ADP

Example: For example, to create the DMZ-2 zone, click **Network > Zone** and then the **Add** icon.

6.6.8 DDNS

Dynamic DNS maps a domain name to a dynamic IP address. The ISG50 helps maintain this mapping.

MENU ITEM(S)	**Configuration > Network > DDNS**
PREREQUISITES	Interface

6.6.9 NAT

Use Network Address Translation (NAT) to make computers on a private network behind the ISG50 available outside the private network.

The ISG50 only checks regular (through-ISG50) firewall rules for packets that are redirected by NAT, it does not check the to-ISG50 firewall rules.

MENU ITEM(S)	**Configuration > Network > NAT**
PREREQUISITES	Interfaces, addresses (HOST)

Example: Suppose you have an FTP server with a private IP address connected to a DMZ port. You could configure a NAT rule to forwards FTP sessions from the WAN to the DMZ.

1. Click **Configuration > Network > NAT** to configure the NAT entry. Add an entry.
2. Name the entry.
3. Select the WAN interface that the FTP traffic is to come in through.
4. Specify the public WAN IP address where the ISG50 will receive the FTP packets.
5. In the **Mapped IP field**, list the IP address of the FTP server. The ISG50 will forward the packets received for the original IP address.
6. In **Mapping Type**, select **Port**.
7. Enter 21 in both the **Original** and the **Mapped Port** fields.

6.6.10 HTTP Redirect

Configure this feature to have the ISG50 transparently forward HTTP (web) traffic to a proxy server. This can speed up web browsing because the proxy server keeps copies of the web pages that have been accessed so they are readily available the next time one of your users needs to access that page.

The ISG50 does not check to-ISG50 firewall rules for packets that are redirected by HTTP redirect. It does check regular (through-ISG50) firewall rules.

MENU ITEM(S)	**Configuration > Network > HTTP Redirect**
PREREQUISITES	Interfaces

Example: Suppose you want HTTP requests from your LAN to go to a HTTP proxy server at IP address 192.168.3.80.

1. Click **Configuration > Network > HTTP Redirect**.
2. Add an entry.
3. Name the entry.
4. Select the interface from which you want to redirect incoming HTTP requests (**lan1**).
5. Specify the IP address of the HTTP proxy server.
6. Specify the port number to use for the HTTP traffic that you forward to the proxy server.

6.6.11 ALG

The ISG50's Application Layer Gateway (ALG) allows VoIP and FTP applications to go through NAT on the ISG50. You can also specify additional signaling port numbers.

MENU ITEM(S)	**Configuration > Network > ALG**

6.6.12 Auth. Policy

Use authentication policies to control who can access the network. You can authenticate users (require them to log in) before they can access the network.

MENU ITEM(S)	**Configuration > Auth. Policy**
PREREQUISITES	Addresses, services, users, authentication methods

6.6.13 Firewall

The firewall controls the travel of traffic between or within zones. You can also configure the firewall to control traffic for NAT (DNAT) and policy routes (SNAT). You can configure firewall rules based on schedules, specific users (or user groups), source or destination addresses (or address groups) and services (or service groups). Each of these objects must be configured in a different screen.

To-ISG50 firewall rules control access to the ISG50. Configure to-ISG50 firewall rules for remote management. By default, the firewall only allows management connections from the LAN or WAN zone.

MENU ITEM(S)	**Configuration > Firewall**
PREREQUISITES	Zones, schedules, users, user groups, addresses (source, destination), address groups (source, destination), services, service groups

Example: Suppose you have a SIP proxy server connected to the DMZ zone for VoIP calls. You could configure a firewall rule to allow VoIP sessions from the SIP proxy server on DMZ to the LAN so VoIP users on the LAN can receive calls.

1 Create a VoIP service object for UDP port 5060 traffic (**Configuration > Object > Service**).

2 Create an address object for the VoIP server (**Configuration > Object > Address**).

3 Click **Configuration > Firewall** to go to the firewall configuration.

4 Select from the **DMZ** zone to the **LAN1** zone, and add a firewall rule using the items you have configured.

- You don't need to specify the schedule or the user.
- In the **Source** field, select the address object of the VoIP server.
- You don't need to specify the destination address.
- Leave the **Access** field set to **Allow** and the **Log** field set to **No**.

Note: The ISG50 checks the firewall rules in order. Make sure each rule is in the correct place in the sequence.

6.6.14 IPSec VPN

Use IPSec VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ISG50 also offers hub-and-spoke VPN.

MENU ITEM(S)	**Configuration > VPN > IPSec VPN**; you can also use the **Quick Setup VPN Setup** wizard.
PREREQUISITES	Interfaces, certificates (authentication), authentication methods (extended authentication), addresses (local network, remote network, NAT), to-ISG50 firewall, firewall
WHERE USED	Policy routes, zones

Example: See Chapter 7 on page 107.

6.6.15 Bandwidth Management

Use bandwidth management (BWM) to configure a BWM rule for a specific IP address, destination port or IP range and specify allowed amounts of bandwidth and priorities.

MENU ITEM(S)	**Configuration > BWM**
PREREQUISITES	Zones

Examples: Suppose you want to give a user named Bob FTP access but with a limited download speed of 200 kbps from LAN (FTP client) to WAN (FTP server).

1. Create user account for Bob.
2. Click **BWM > Add New Policy**. Select the user account that you created for Bob.
3. Select from LAN zone to WAN zone (default).
4. Set BWM inbound value to 200kbps and keep the default values for all other fields.

6.6.16 ADP

Use ADP to detect and take action on traffic and protocol anomalies.

MENU ITEM(S)	**Configuration > Anti-X > ADP**
PREREQUISITES	Zones

6.7 Objects

Objects store information and are referenced by other features. If you update this information in response to changes, the ISG50 automatically propagates the change through the features that use the object. Move your cursor over a configuration object that has a magnifying-glass icon (such as a user group, address, address group, service, service group, zone, or schedule) to display basic information about the object.

The following table introduces the objects. You can also use this table when you want to delete an object because you have to delete references to the object first.

Table 16 Objects Overview

OBJECT	WHERE USED
user/group	See the User/Group section for details on users and user groups.
address	VPN connections (local / remote network, NAT), policy routes (criteria, next-hop [HOST], NAT), authentication policies, firewall, NAT (HOST), user settings (force user authentication), address groups, remote management (System)
address group	Policy routes (criteria), firewall, user settings (force user authentication), address groups, remote management (System)
service, service group	Policy routes (criteria, port triggering), firewall, service groups, log (criteria)
schedule	Policy routes (criteria), authentication policies, firewall, user settings (force user authentication)
AAA server	Authentication methods
authentication methods	VPN gateways (extended authentication), WWW (client authentication)
certificates	VPN gateways, WWW, SSH, FTP

6.7.1 User/Group

Use these screens to configure the ISG50's administrator and user accounts. The ISG50 provides the following user types.

Table 17 User Types

TYPE	ABILITIES
admin	Change ISG50 configuration (web, CLI)
limited-admin	Look at ISG50 configuration (web)
user	Access network services, browse user-mode commands (CLI)
guest	Access network services
ext-user	The same as a user or a guest except the ISG50 looks for the specific type in an external authentication server. If the type is not available, the ISG50 applies default settings.
ext-group-user	External group user account.

If you want to force users to log in to the ISG50 before the ISG50 routes traffic for them, you might have to configure prerequisites first.

MENU ITEM(S)	**Object > User/Group**
PREREQUISITES	Addresses, address groups, schedules. The prerequisites are only used in policies to force user authentication
WHERE USED	Policy routes, firewall, user groups, VPN

6.8 System

This section introduces some of the management features in the ISG50. Use **Host Name** to configure the system and domain name for the ISG50. Use **Date/Time** to configure the current date, time, and time zone in the ISG50. Use **Console Speed** to set the console speed. Use **Language** to select a language for the Web Configurator screens.

6.8.1 DNS, WWW, SSH, TELNET, FTP, SNMP

Use these screens to set which services or protocols can be used to access the ISG50 through which zone and from which addresses (address objects) the access can come.

MENU ITEM(S)	**Configuration > System > DNS, WWW, SSH, TELNET, FTP, SNMP, Language**
PREREQUISITES	To-ISG50 firewall, zones, addresses, address groups, certificates (WWW, SSH, FTP), authentication methods (WWW)

Example: Suppose you want to allow an administrator to use HTTPS to manage the ISG50 from the WAN.

1. Create an administrator account (**Configuration > Object > User/Group**).

2. Create an address object for the administrator's computer (**Configuration > Object > Address**).

3 Click **Configuration > System > WWW** to configure the HTTP management access. Enable HTTPS and add an administrator service control entry.

- Select the address object for the administrator’s computer.
- Select the **WAN** zone.
- Set the action to **Accept**.

6.8.2 Logs and Reports

The ISG50 provides a system log, offers two e-mail profiles to which to send log messages, and sends information to four syslog servers. It can also e-mail you statistical reports on a daily basis. It can also record a CDR and e-mail alerts.

MENU ITEM(S)	**Configuration > Log & Report**

6.8.3 File Manager

Use these screens to upload, download, delete, or run scripts of CLI commands. You can manage

- Configuration files. Use configuration files to back up and restore the complete configuration of the ISG50. You can store multiple configuration files in the ISG50 and switch between them without restarting.
- Shell scripts. Use shell scripts to run a series of CLI commands. These are useful for large, repetitive configuration changes (for example, creating a lot of VPN tunnels) and for troubleshooting.

You can edit configuration files and shell scripts in any text editor.

MENU ITEM(S)	**Maintenance > File Manager**

6.8.4 Diagnostics

The ISG50 can generate a file containing the ISG50’s configuration and diagnostic information. It can also capture packets going through the ISG50’s interfaces so you can analyze them to identify network problems.

MENU ITEM(S)	**Maintenance > Diagnostics**

6.8.5 Shutdown

Use this to shutdown the device in preparation for disconnecting the power.

Always use Maintenance > Shutdown > Shutdown or the shutdown command before you turn off the ISG50 or remove the power. Not doing so can cause the firmware to become corrupt.

MENU ITEM(S)	**Maintenance > Shutdown**

General Tutorials

Here are examples of using the Web Configurator to configure general settings in the ISG50. See Chapter 8 on page 135 for how to configure PBX settings.

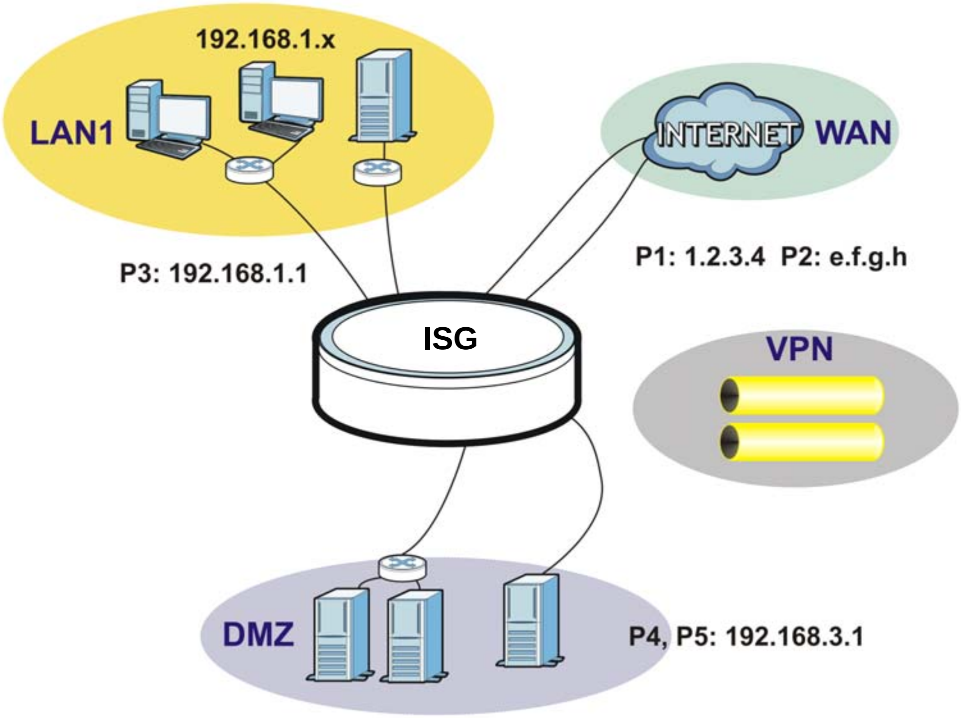
Note: The tutorials featured here require a basic understanding of connecting to and using the Web Configurator, see Chapter 3 on page 43 for details. For field descriptions of individual screens, see Technical Reference on page 183.

7.1 How to Configure Interfaces, Port Roles, and Zones

This tutorial shows how to configure Ethernet interfaces, port roles, and zones for the following example configuration (see Section 6.3.2 on page 93 for the default configuration).

- You want to be able to apply security settings specifically for all VPN tunnels so you add them to the IPSec_VPN zone.
- The **wan1** interface uses a static IP address of 1.2.3.4.
- Add **P4** to the **dmz** interface. The **dmz** interface is used for a protected local network. It uses IP address 192.168.3.1 and has a DHCP server.

Figure 71 Ethernet Interface, Port Roles, and Zone Configuration Example

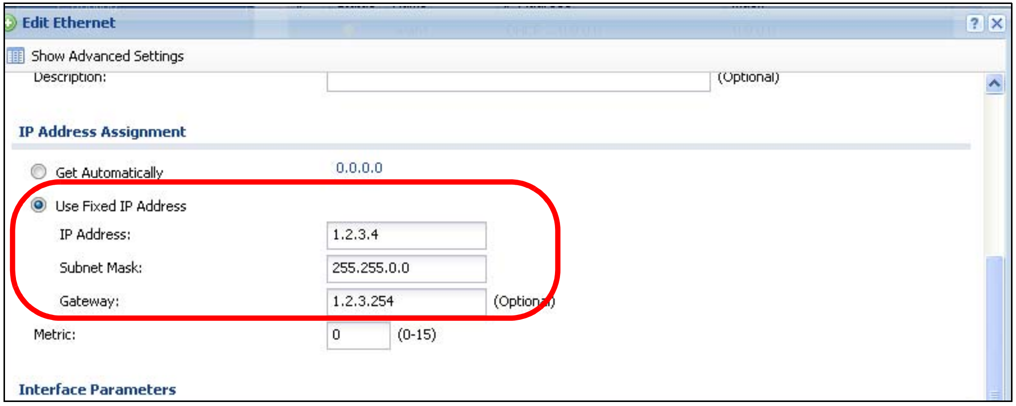


7.1.1 Configure a WAN Ethernet Interface

You need to assign the ISG50's **wan1** interface a static IP address of 1.2.3.4.

Click **Configuration > Network > Interface > Ethernet** and double-click the **wan1** interface's entry. Select **Use Fixed IP Address** and configure the IP address, subnet mask, and default gateway settings and click **OK**.

Figure 72 Configuration > Network > Interface > Ethernet > Edit wan1


Edit Ethernet
Show Advanced Settings
IP Address Assignment
Interface Parameters

Description: (Optional)

○ Get Automatically 0.0.0.0

● Use Fixed IP Address

IP Address: 1.2.3.4

Subnet Mask: 255.255.0.0

Gateway: 1.2.3.254 (Optional)

Metric: 0 (0-15)

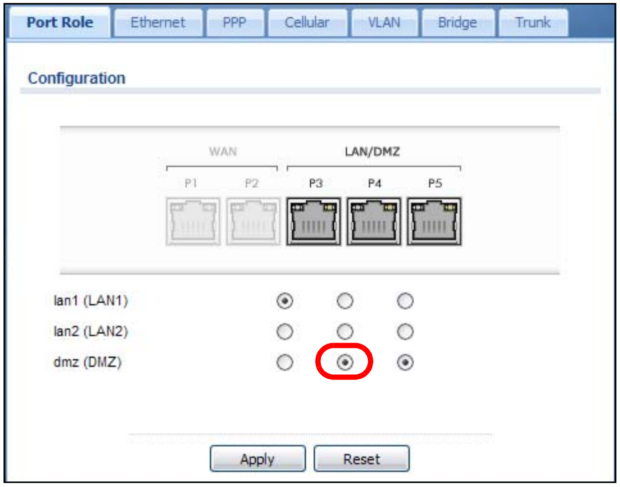
7.1.2 Configure Port Roles

Here is how to take the **P4** port from the lan2 interface and add it to the dmz interface.

1 Click **Configuration > Network > Interface > Role**.

2 Under **P4** select the **dmz (DMZ)** radio button and click **Apply**.

Figure 73 Configuration > Network > Interface > Port Roles Example


Port Role
Ethernet
PPP
Cellular
VLAN
Bridge
Trunk
Configuration
WAN
LAN/DMZ
P1
P2
Apply
Reset

	P3	P4	P5
lan1 (LAN1)	●	○	○
lan2 (LAN2)	○	○	○
dmz (DMZ)	○	●	●

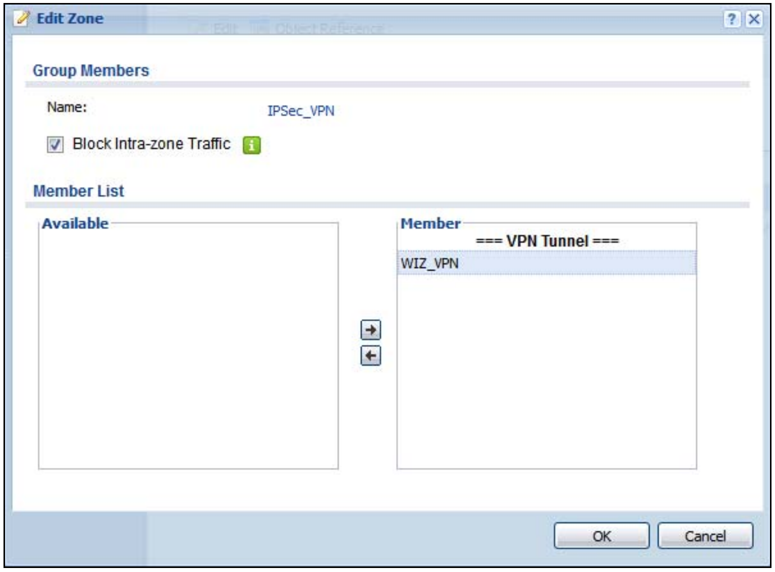
7.1.3 Configure Zones

Do the following to create a VPN zone.

1 Click **Configuration > Network** > **Zone** and then double-click the **IPSec_VPN** entry.

2 Select **WIZ_VPN** and move it to the **Member** box and click **OK**.

Figure 74 Configuration > Network > Zone > IPSec_VPN Edit



Edit Zone
Group Members
Member List
Available
OK
Cancel

Name: IPSec_VPN

☑ Block Intra-zone Traffic

Member
=== VPN Tunnel ===
WIZ_VPN

7.2 How to Configure a Cellular Interface

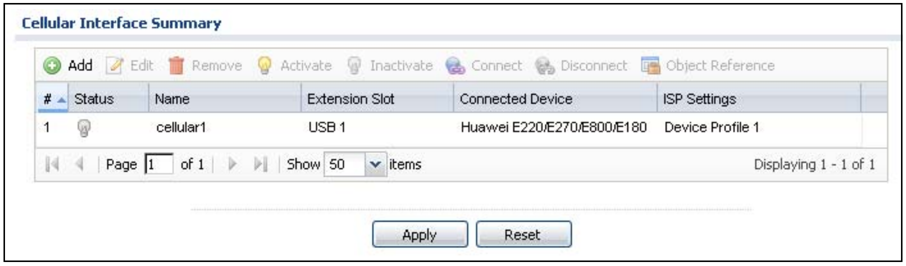
Use 3G cards for cellular WAN (Internet) connections. See www.zyxel.com for a list of the compatible 3G devices. In this example you connect the 3G USB card before you configure the cellular interfaces but is also possible to reverse the sequence.

1 Make sure the 3G device’s SIM card is installed.

2 Connect the 3G device to one of the ISG50’s USB ports.

3 Click **Configuration > Network > Interface > Cellular**. Select the 3G device’s entry and click **Edit**.

Figure 75 Configuration > Network > Interface > Cellular

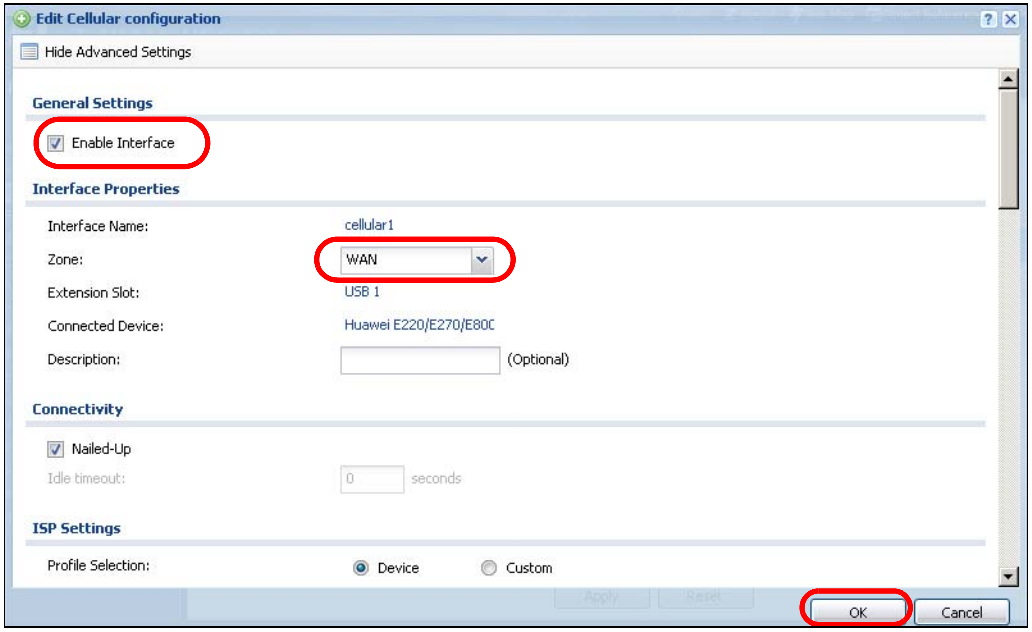


Cellular Interface Summary
Add
Edit
Remove
Activate
Inactivate
Connect
Disconnect
Object Reference
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Apply
Reset

#	Status	Name	Extension Slot	Connected Device	ISP Settings
1		cellular1	USB 1	Huawei E220/E270/E800/E180	Device Profile 1

4 Enable the interface and add it to a zone. It is highly recommended that you set the **Zone** to **WAN** to apply your WAN zone security settings to this 3G connection. Leaving **Zone** set to **none** has the ISG50 not apply any security settings to the 3G connection. Enter the **PIN Code** provided by the cellular 3G service provider (0000 in this example).

Figure 76 Configuration > Network > Interface > Cellular > Edit



Edit Cellular configuration

Hide Advanced Settings

General Settings

☑ Enable Interface

Interface Properties

Interface Name: cellular1

Zone: WAN

Extension Slot: USB 1

Connected Device: Huawei E220/E270/E80C

Description: (Optional)

Connectivity

☑ Nailed-Up

Idle timeout: 0 seconds

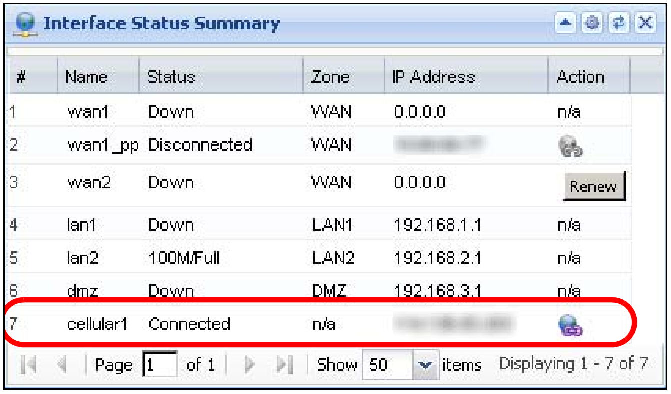
ISP Settings

Profile Selection: ● Device ○ Custom

Note: The **Network Selection** is set to **Auto** by default. This means that the 3G USB modem may connect to another 3G network when your service provider is not in range or when necessary. Select **Home** to have the 3G device connect only to your home network or local service provider. This prevents you from being charged using the rate of a different ISP.

5 Go to the **Dashboard**. The **Interface Status Summary** section should contain a “cellular” entry. When its connection status is **Connected** you can use the 3G connection to access the Internet.

Figure 77 Status



Interface Status Summary

#	Name	Status	Zone	IP Address	Action
1	wan1	Down	WAN	0.0.0.0	n/a
2	wan1_pp	Disconnected	WAN	[redacted]	
3	wan2	Down	WAN	0.0.0.0	Renew
4	lan1	Down	LAN1	192.168.1.1	n/a
5	lan2	100M/Full	LAN2	192.168.2.1	n/a
6	dmz	Down	DMZ	192.168.3.1	n/a
7	cellular1	Connected	n/a	[redacted]	

6 The ISG50 automatically adds the cellular interface to the system default WAN trunk. If the ISG50 is using a user-configured trunk as its default trunk and you want this cellular interface to be part of it, use the **Trunk** screens to add it.

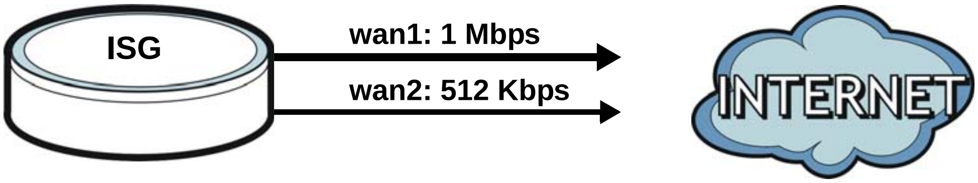
This way the ISG50 can automatically balance the traffic load amongst the available WAN connections to enhance overall network throughput. Plus, if a WAN connection goes down, the ISG50 still sends traffic through the remaining WAN connections. For a simple test, disconnect all of the ISG50’s wired WAN connections. If you can still access the Internet, your cellular interface is properly configured and your cellular device is working.

To fine-tune the load balancing configuration, see Chapter 13 on page 281. See also Section 7.3 on page 111 for an example.

7.3 How to Configure Load Balancing

This example shows how to configure a trunk for two WAN connections (to the Internet). The available bandwidth for the connections is 1Mbps (**wan1**) and 512 Kbps (**wan2**) respectively. As these connections have different bandwidth, use the **Weighted Round Robin** algorithm to send traffic to wan1 and wan2 in a 2:1 ratio.

Figure 78 Trunk Example



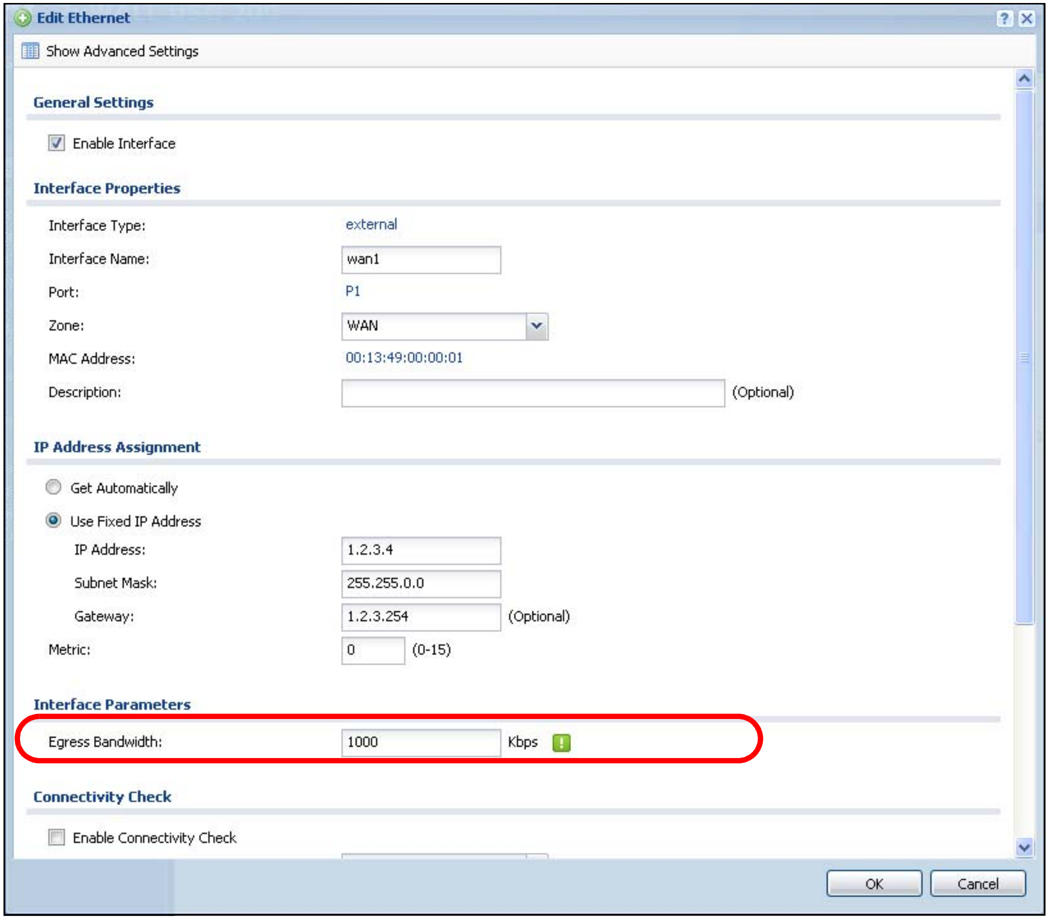
You do not have to change many of the ISG50's settings from the defaults to set up this trunk. You only have to set up the outgoing bandwidth on each of the WAN interfaces and configure the WAN_TRUNK trunk's load balancing settings.

7.3.1 Set Up Available Bandwidth on Ethernet Interfaces

Here is how to set a limit on how much traffic the ISG50 tries to send out through each WAN interface.

1. Click **Configuration > Network > Interface > Ethernet** and double-click the **wan1** entry. Enter the available bandwidth (1000 kbps) in the **Egress Bandwidth** field. Click **OK**.

Figure 79 Configuration > Network > Interface > Ethernet > Edit (wan1)



General Settings

☑ Enable Interface

Interface Properties

Interface Type: external
Interface Name: wan1
Port: P1
Zone: WAN
MAC Address: 00:13:49:00:00:01
Description: (Optional)

IP Address Assignment

○ Get Automatically
● Use Fixed IP Address
IP Address: 1.2.3.4
Subnet Mask: 255.255.0.0
Gateway: 1.2.3.254 (Optional)
Metric: 0 (0-15)

Interface Parameters

Egress Bandwidth: 1000 Kbps

Connectivity Check

☐ Enable Connectivity Check

2 Repeat the process to set the egress bandwidth for **wan2** to 512 Kbps.

7.3.2 Configure the WAN Trunk

1 Click **Configuration > Network > Interface > Trunk**. Click the **Add** icon.

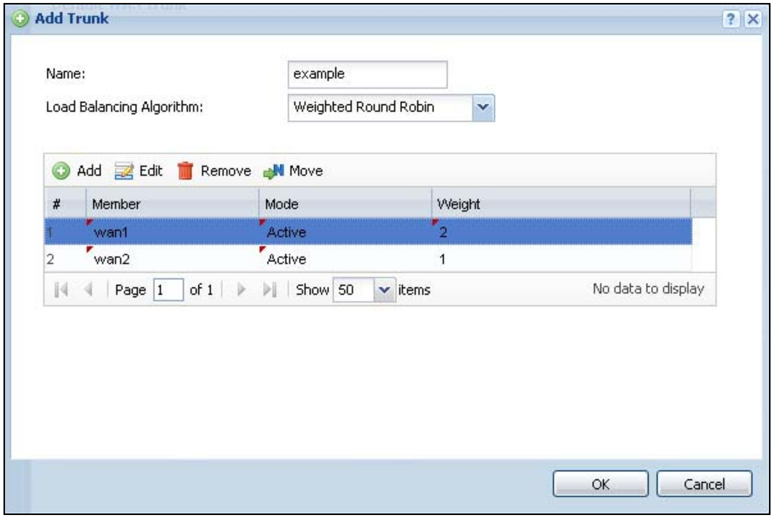
2 Name the trunk and set the **Load Balancing Algorithm** field to **Weighted Round Robin**.

Add **wan1** and enter 2 in the **Weight** column.

Add **wan2** and enter 1 in the **Weight** column.

Click **OK**.

Figure 80   Configuration > Network > Interface > Trunk > Add


Add Trunk
Add
Edit
Remove
Move
OK
Cancel

Name: example

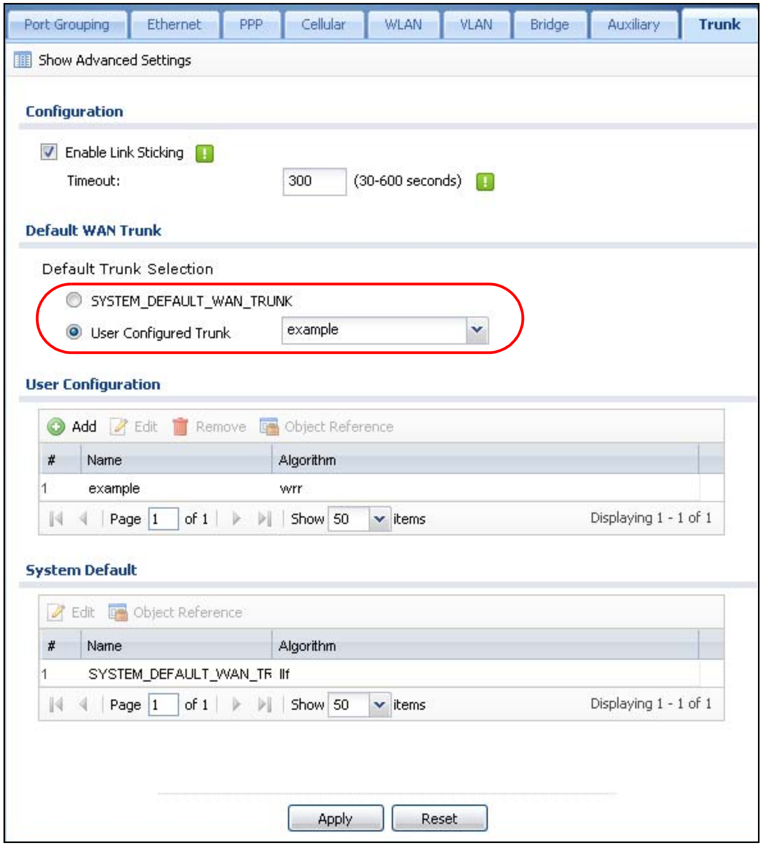
Load Balancing Algorithm: Weighted Round Robin

#	Member	Mode	Weight
1	wan1	Active	2
2	wan2	Active	1

Page 1 of 1 Show 50 items No data to display

3 Select the trunk as the default trunk and click **Apply**.

Figure 81   Configuration > Network > Interface > Trunk


Port Grouping
Ethernet
PPP
Cellular
WLAN
VLAN
Bridge
Auxiliary
Trunk
Show Advanced Settings
Add
Edit
Remove
Object Reference
Apply
Reset

Configuration

☑ Enable Link Sticking

Timeout: 300 (30-600 seconds)

Default WAN Trunk

Default Trunk Selection

○ SYSTEM_DEFAULT_WAN_TRUNK

● User Configured Trunk example

User Configuration

#	Name	Algorithm
1	example	wrr

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

System Default

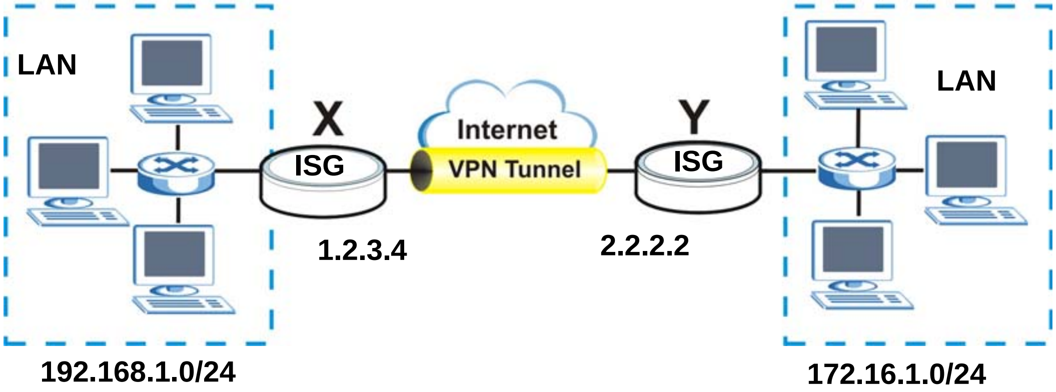
#	Name	Algorithm
1	SYSTEM_DEFAULT_WAN_TR	llf

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

7.4 How to Set Up an IPSec VPN Tunnel

This example shows how to use the IPSec VPN configuration screens to create the following VPN tunnel, see Section 5.4 on page 77 for details on the VPN quick setup wizard.

Figure 82 VPN Example



In this example, the ISG50 is router **X** (1.2.3.4), and the remote IPSec router is router **Y** (2.2.2.2). Create the VPN tunnel between ISG50 **X**'s LAN subnet (192.168.1.0/24**)** and the LAN subnet behind peer IPSec router **Y** (172.16.1.0/24).

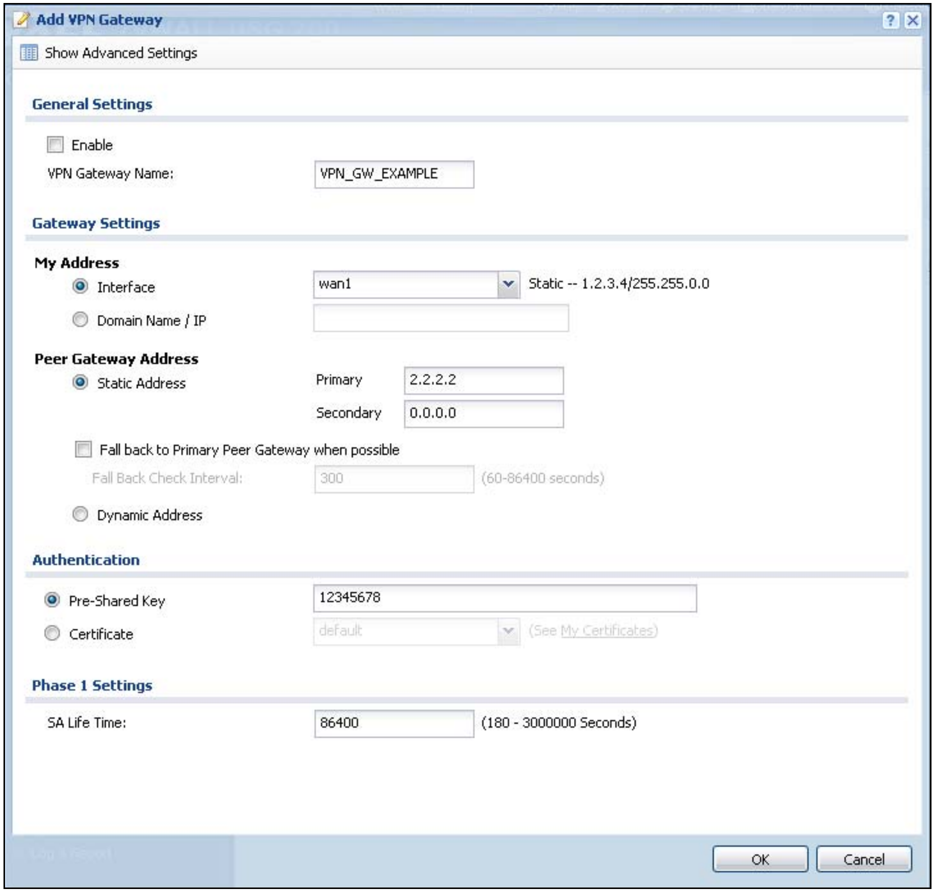
7.4.1 Set Up the VPN Gateway

The VPN gateway manages the IKE SA. You do not have to set up any other objects before you configure the VPN gateway because this VPN tunnel does not use any certificates or extended authentication.

1 Click **Configuration > VPN > IPSec VPN > VPN Gateway**, and then click the **Add** icon.

2 Enable the VPN gateway and name it ("VPN_GW_EXAMPLE"). For **My Address**, select **Interface** and **wan1**. For the **Peer Gateway Address**, select **Static Address** and enter 2.2.2.2 in the **Primary** field. For the **Authentication**, Select **Pre-Shared Key** and enter 12345678. Click **OK**.

Figure 83 Configuration > VPN > IPSec VPN > VPN Gateway > Add


Add VPN Gateway
Show Advanced Settings
General Settings
Gateway Settings
Authentication
Phase 1 Settings
OK
Cancel

☐ Enable

VPN Gateway Name: VPN_GW_EXAMPLE

My Address

● Interface: wan1 — Static -- 1.2.3.4/255.255.0.0

○ Domain Name / IP

Peer Gateway Address

● Static Address — Primary: 2.2.2.2 — Secondary: 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

○ Dynamic Address

● Pre-Shared Key: 12345678

○ Certificate: default (See My Certificates)

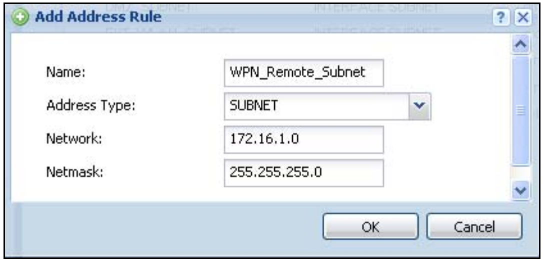
SA Life Time: 86400 (180 - 3000000 Seconds)

7.4.2 Set Up the VPN Connection

The VPN connection manages the IPSec SA. You have to set up the address objects for the local network and remote network before you can set up the VPN connection.

1. Click **Configuration > Object > Address**. Click the **Add** icon.
2. Give the new address object a name ("VPN_REMOTE_SUBNET"), change the **Address Type** to **SUBNET**. Set up the **Network** field to 172.16.1.0 and the **Netmask** to 255.255.255.0. Click **OK**.

Figure 84 Configuration > Object > Address > Add


Add Address Rule
OK
Cancel

Name: WPN_Remote_Subnet

Address Type: SUBNET

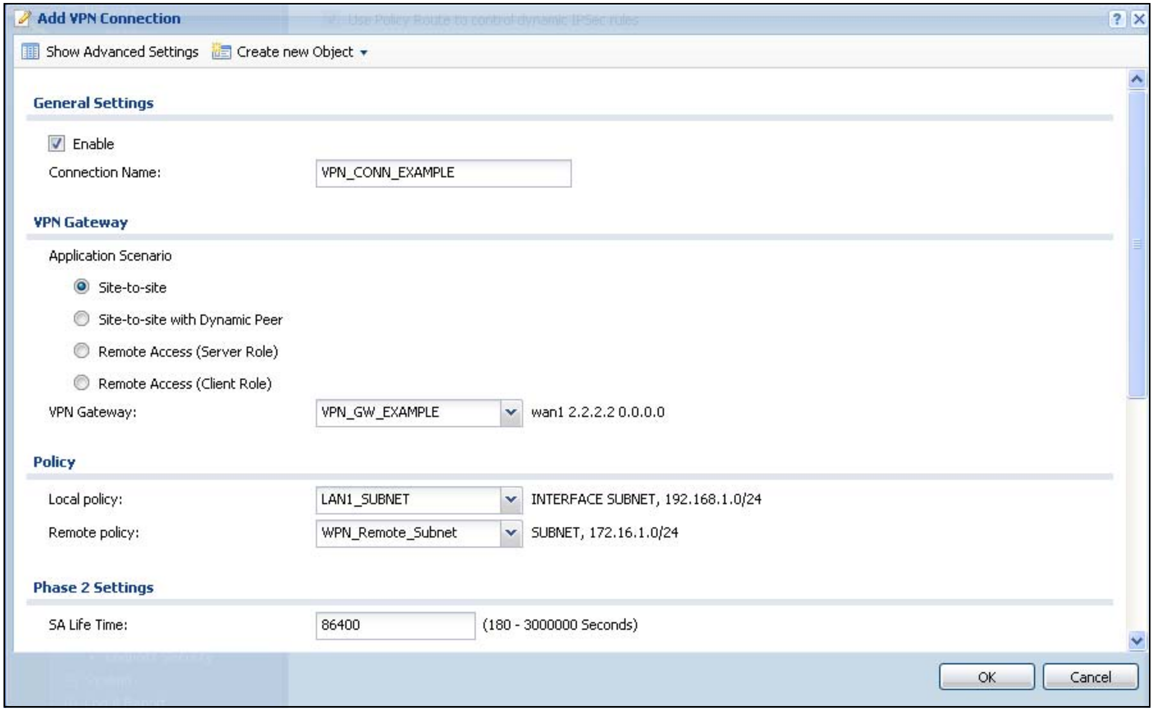
Network: 172.16.1.0

Netmask: 255.255.255.0

3. Click **Configuration > VPN > IPSec VPN > VPN Connection**. Click the **Add** icon.

4 Enable the VPN connection and name it ("VPN_CONN_EXAMPLE"). Under **VPN Gateway** select **Site-to-site** and the VPN gateway (**VPN_GW_EXAMPLE**). Under **Policy**, select **LAN1_SUBNET** for the local network and **VPN_REMOTE_SUBNET** for the remote. Click **OK**.

Figure 85 Configuration > VPN > IPSec VPN > VPN Connection > Add



☑ Enable
Connection Name: VPN_CONN_EXAMPLE
Application Scenario
● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)
VPN Gateway: VPN_GW_EXAMPLE wan1 2.2.2.2 0.0.0.0
Local policy: LAN1_SUBNET INTERFACE SUBNET, 192.168.1.0/24
Remote policy: WPN_Remote_Subnet SUBNET, 172.16.1.0/24
SA Life Time: 86400 (180 - 3000000 Seconds)

5 Now set up the VPN settings on the peer IPSec router and try to establish the VPN tunnel. To trigger the VPN, either try to connect to a device on the peer IPSec router's LAN or click **Configuration > VPN > IPSec VPN > VPN Connection** and use the VPN connection screen's **Connect** icon.

7.4.3 Configure Security Policies for the VPN Tunnel

You configure security policies based on zones. The new VPN connection was assigned to the IPSec_VPN zone. By default, there are no security restrictions on the IPSec_VPN zone, so, next, you should set up security policies (firewall rules, ADP, and so on) that apply to the IPSec_VPN zone. Make sure all firewalls between the ISG50 and remote IPSec router allow UDP port 500 (IKE) and IP protocol 50 (AH) or 51 (ESP). If you enable NAT traversal, all firewalls between the ISG50 and remote IPSec router should also allow UDP port 4500.

7.5 How to Configure User-aware Access Control

You can configure many policies and security settings for specific users or groups of users. This is illustrated in the following example, where you will set up the following policies. This is a simple example that does not include priorities for different types of traffic. See Chapter 25 on page 397 for more on bandwidth management.

Table 18 User-aware Access Control Example

GROUP (USER)	WEB SURFING	WEB BANDWIDTH	MSN	LAN1-TO-DMZ ACCESS
Finance (Leo)	Yes	200K	No	Yes
Engineer (Steven)	Yes	100K	No	No
Sales (Debbie)	Yes	100K	Yes (M-F, 08:30~18:00)	Yes
Boss (Andy)	Yes	100K	Yes	Yes
Guest (guest)	Yes	50K	No	No
Others	No	---	No	No

The users are authenticated by an external RADIUS server at 192.168.1.200.

First, set up the user accounts and user groups in the ISG50. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

The ISG50 has its default settings.

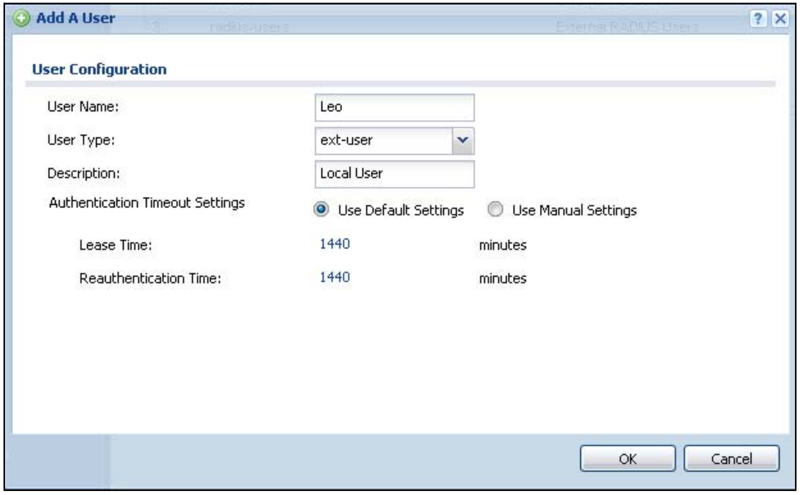
7.5.1 Set Up User Accounts

Set up one user account for each user account in the RADIUS server. If it is possible to export user names from the RADIUS server to a text file, then you might create a script to create the user accounts instead. This example uses the Web Configurator.

1 Click **Configuration > Object > User/Group > User**. Click the **Add** icon.

2 Enter the same user name that is used in the RADIUS server, and set the **User Type** to **ext-user** because this user account is authenticated by an external server. Click **OK**.

Figure 86 Configuration > Object > User/Group > User > Add



User Name: Leo

User Type: ext-user

Description: Local User

Authentication Timeout Settings: ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

3 Repeat this process to set up the remaining user accounts.

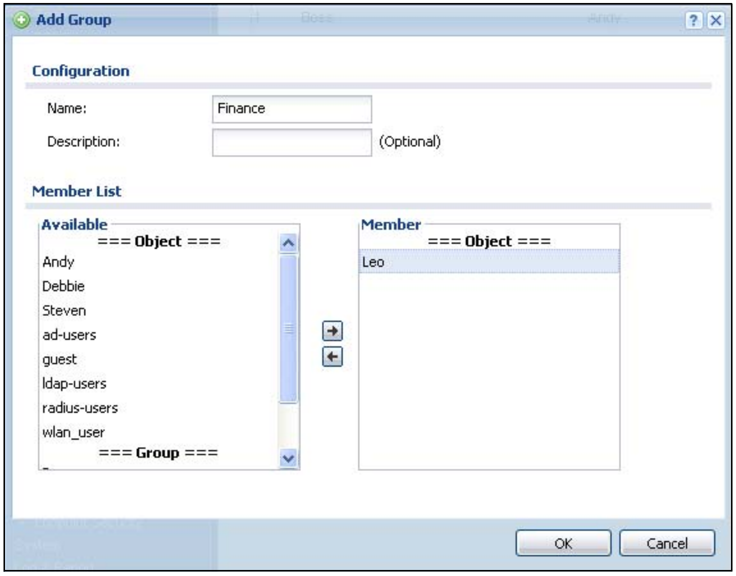
7.5.2 Set Up User Groups

Set up the user groups and assign the users to the user groups.

1 Click **Configuration > Object > User/Group > Group**. Click the **Add** icon.

2 Enter the name of the group that is used in the example in Table 18 on page 117. In this example, it is “Finance”. Then, select **User/Leo** and click the right arrow to move him to the **Member** list. This example only has one member in this group, so click **OK**. Of course you could add more members later.

Figure 87 Configuration > Object > User/Group > Group > Add



Name: Finance

Description: (Optional)

Member: Leo

Add Group
Configuration
Member List
Available
=== Object ===
Andy
Debbie
Steven
ad-users
guest
ldap-users
radius-users
wlan_user
=== Group ===
Member
=== Object ===
OK
Cancel

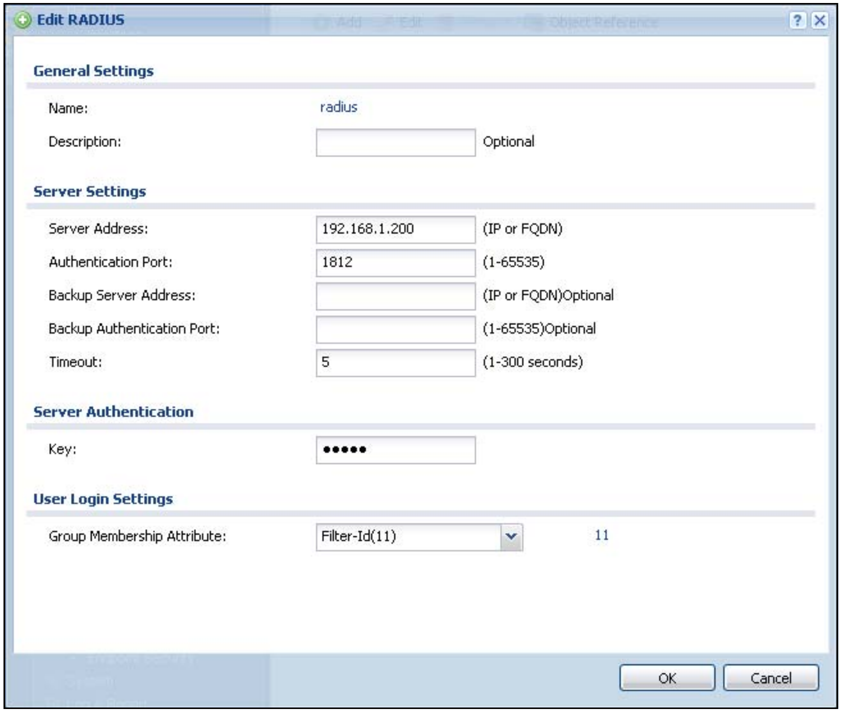
3 Repeat this process to set up the remaining user groups.

7.5.3 Set Up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the ISG50 to use the authentication method. Finally, force users to log in to the ISG50 before it routes traffic for them.

1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Configure the RADIUS server’s address authentication port (1812 if you were not told otherwise), key, and click **Apply**.

Figure 88 Configuration > Object > AAA Server > RADIUS > Add



General Settings

Name: radius

Description: Optional

Server Settings

Server Address: 192.168.1.200 (IP or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN)Optional

Backup Authentication Port: (1-65535)Optional

Timeout: 5 (1-300 seconds)

Server Authentication

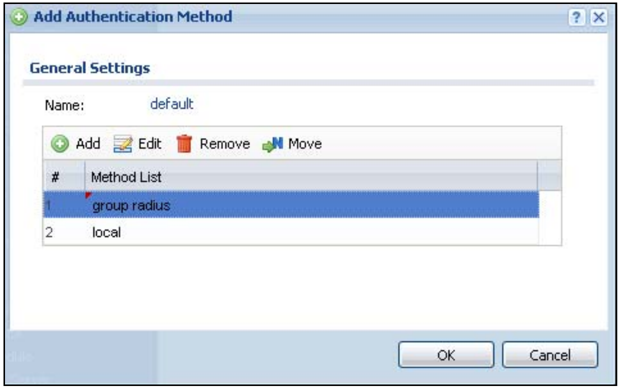
Key: •••••

User Login Settings

Group Membership Attribute: Filter-Id(11) 11

2 Click **Configuration > Object > Auth. method**. Double-click the **default** entry. Click the **Add** icon. Select **group radius** because the ISG50 should use the specified RADIUS server for authentication. Click **OK**.

Figure 89 Configuration > Object > Auth. method > Add



General Settings

Name: default

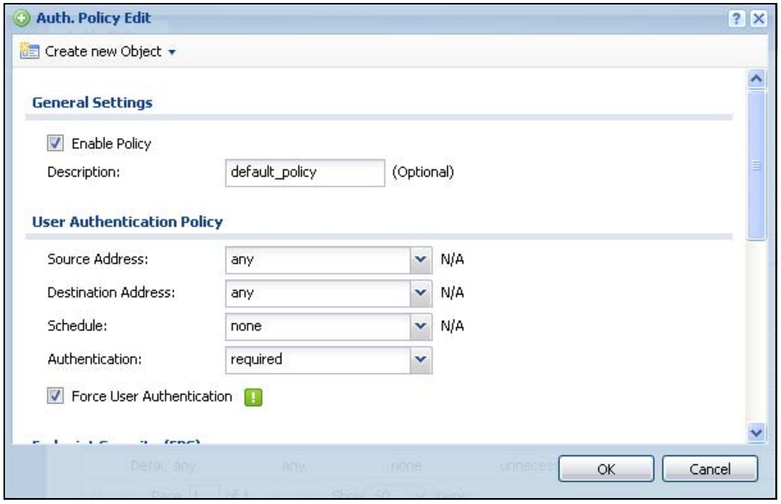
#	Method List
1	group radius
2	local

3 Click **Configuration > Auth. Policy**. In the **Authentication Policy Summary** section, click the **Add** icon.

4 Set up a default policy that forces every user to log in to the ISG50 before the ISG50 routes traffic for them. Select **Enable**. Set the **Authentication** field to **required**, and make sure **Force User Authentication** is selected. Keep the rest of the default settings, and click **OK**.

Note: The users will have to log in using the Web Configurator login screen before they can use HTTP or MSN.

Figure 90 Configuration > Object > User/Group > Setting > Add (Force User Authentication Policy)



☑ Enable Policy

Description: default_policy (Optional)

Source Address: any N/A

Destination Address: any N/A

Schedule: none N/A

Authentication: required

☑ Force User Authentication

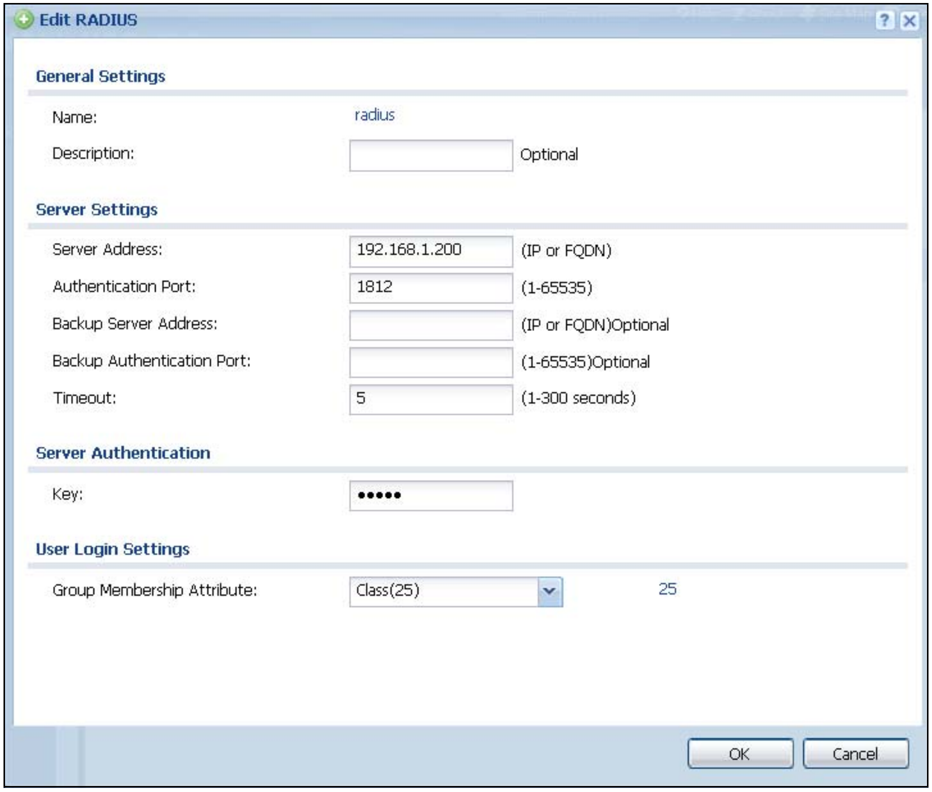
When the users try to browse the web (or use any HTTP/HTTPS application), the **Login** screen appears. They have to log in using the user name and password in the RADIUS server.

7.6 How to Use a RADIUS Server to Authenticate User Accounts Based on Groups

The previous example showed how to have a RADIUS server authenticate individual user accounts. If the RADIUS server has different user groups distinguished by the value of a specific attribute, you can configure the make a couple of slight changes in the configuration to have the RADIUS server authenticate groups of user accounts defined in the RADIUS server.

1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Besides configuring the RADIUS server’s address, authentication port, and key; set the **Group Membership Attribute** field to the attribute that the ISG50 is to check to determine to which group a user belongs. This example uses **Class**. This attribute’s value is called a group identifier; it determines to which group a user belongs. In this example the values are Finance, Engineer, Sales, and Boss.

Figure 91 Configuration > Object > AAA Server > RADIUS > Add



General Settings

Name: radius

Description: Optional

Server Settings

Server Address: 192.168.1.200 (IP or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN)Optional

Backup Authentication Port: (1-65535)Optional

Timeout: 5 (1-300 seconds)

Server Authentication

Key: •••••

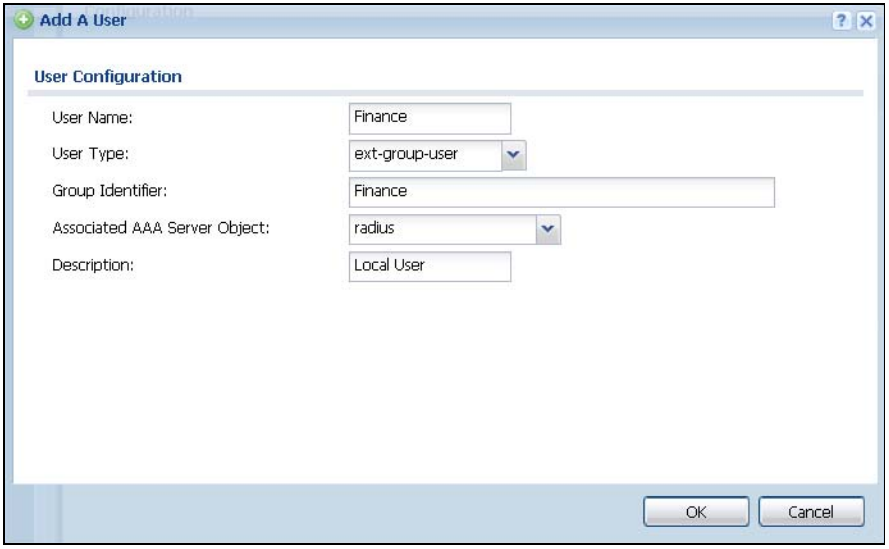
User Login Settings

Group Membership Attribute: Class(25) 25

2 Now you add ext-group-user user objects to identify groups based on the group identifier values. Set up one user account for each group of user accounts in the RADIUS server. Click **Configuration > Object > User/Group > User**. Click the **Add** icon.

Enter a user name and set the **User Type** to **ext-group-user**. In the **Group Identifier** field, enter Finance, Engineer, Sales, or Boss and set the Associated AAA Server Object to radius.

Figure 92 Configuration > Object > User/Group > User > Add



User Configuration

User Name: Finance

User Type: ext-group-user

Group Identifier: Finance

Associated AAA Server Object: radius

Description: Local User

3 Repeat this process to set up the remaining groups of user accounts.

7.7 How to Use Authentication Policies

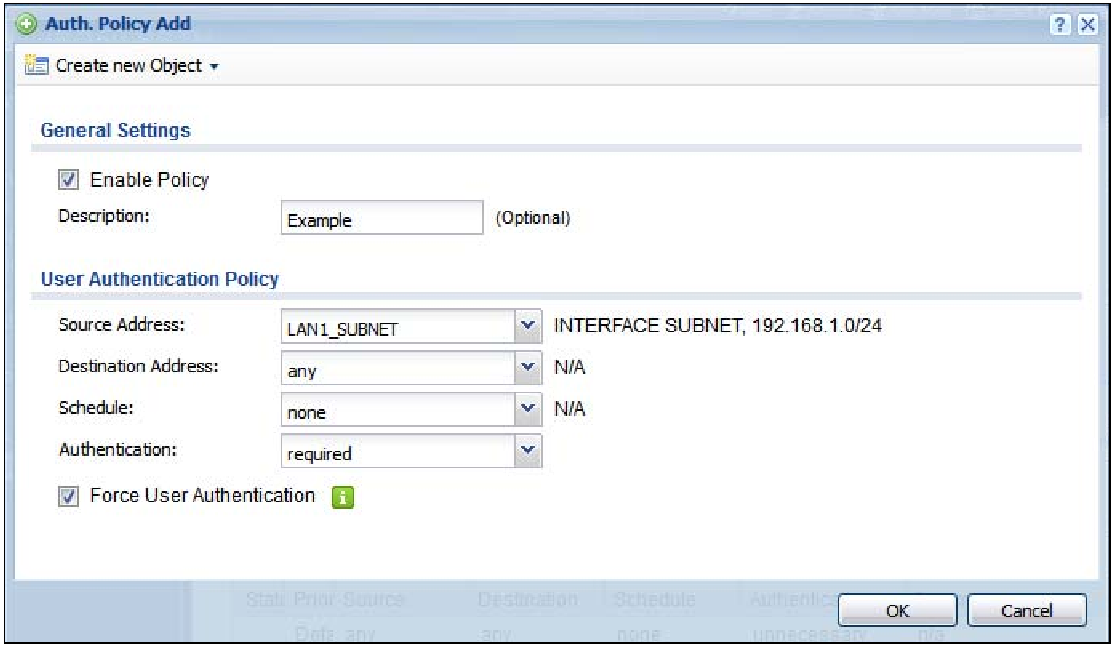
Here is how to use authentication policies to make sure that users log in before they are allowed to access the network.

7.7.1 Configure the Authentication Policy

Click **Configuration > Auth. Policy** and then the **Authentication Policy Summary**'s **Add** icon to open the **Auth. Policy Edit** screen. Use this screen to configure an authentication policy.

- Enable the policy and name it.
- Set the **Source Address** to LAN1 and the **Destination Address** to **any**, the **Schedule** set to **none**, and **Authentication** set to **required** to apply this policy to all users.
- Select **Force User Authentication** to redirect the HTTP traffic of users who are not yet logged in to the ISG50's login screen.
- Click **OK**.

Figure 93 Configuration > Auth. Policy > Add



☑ Enable Policy

Description: Example (Optional)

Source Address: LAN1_SUBNET INTERFACE SUBNET, 192.168.1.0/24

Destination Address: any N/A

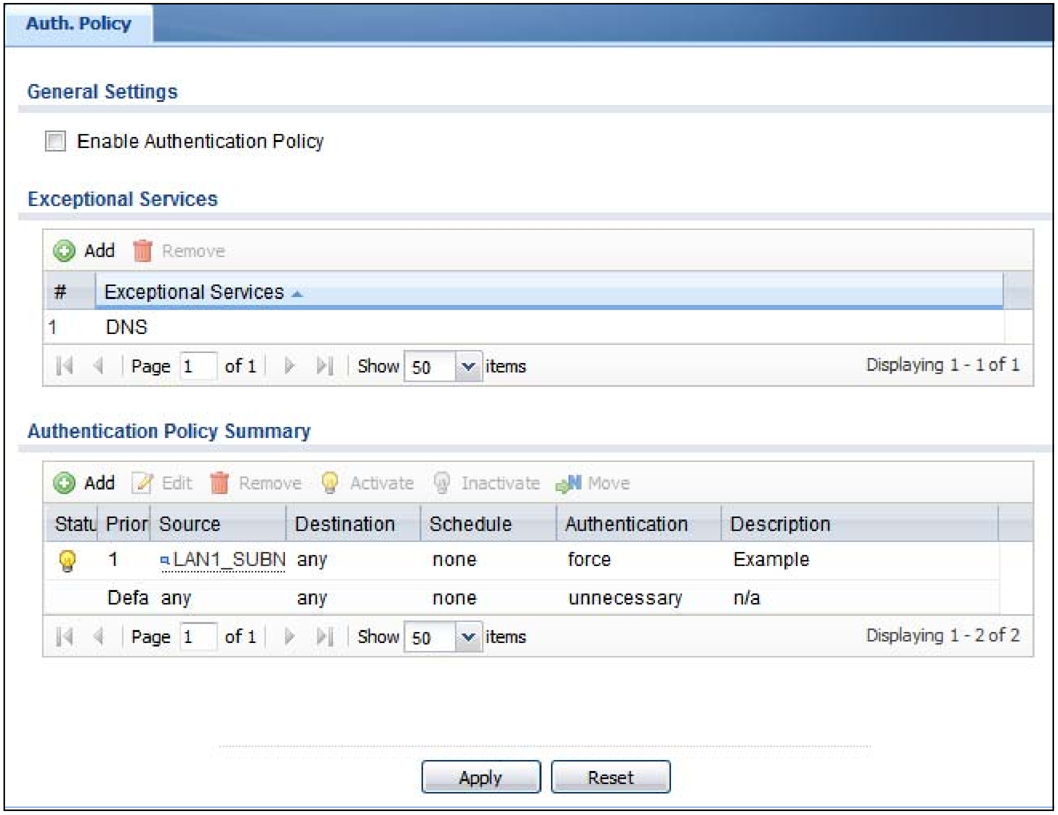
Schedule: none N/A

Authentication: required

☑ Force User Authentication

4 Turn on authentication policy and click **Apply**.

Figure 94   Configuration > Auth. Policy


Auth. Policy
General Settings
Exceptional Services
Add
Remove
Authentication Policy Summary
Add
Edit
Remove
Activate
Inactivate
Move
Apply
Reset

☐ Enable Authentication Policy

#	Exceptional Services
1	DNS

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Statu	Prior	Source	Destination	Schedule	Authentication	Description
💡	1	LAN1_SUBN	any	none	force	Example
	Defa	any	any	none	unnecessary	n/a

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

7.8 How to Configure Service Control

Service control lets you configure rules that control HTTP and HTTPS management access (to the Web Configurator) and separate rules that control HTTP and HTTPS user access. See Chapter 52 on page 665 for more on service control.

The To-ISG50 firewall rules apply to any kind of HTTP or HTTPS connection to the ISG50. They do not distinguish between administrator management access and user access. If you configure service control to allow management or user HTTP or HTTPS access, make sure the firewall is not configured to block that access.

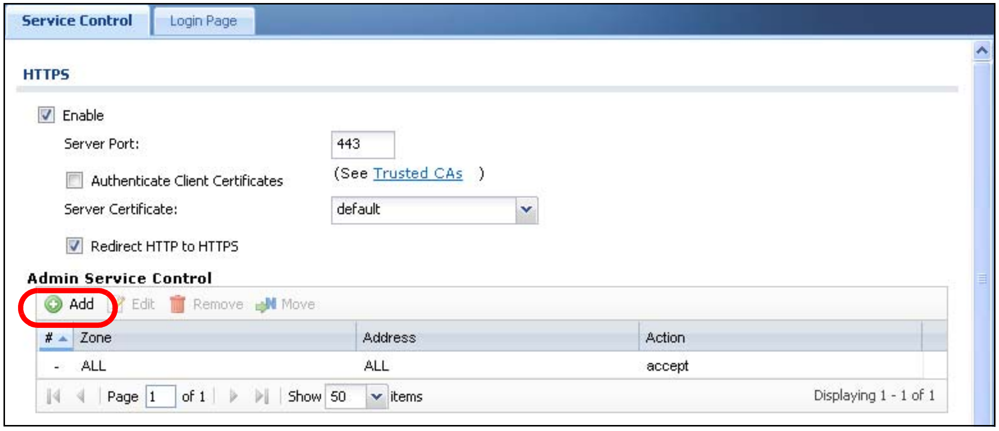
7.8.1 Allow HTTPS Administrator Access Only From the LAN

This example configures service control to block administrator HTTPS access from all zones except the LAN1.

1 Click **Configuration > System > WWW**.

2 In HTTPS **Admin Service Control,** click the **Add** icon.

Figure 95 Configuration > System > WWW


Service Control
Login Page
Add
Edit
Remove
Move
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1

HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

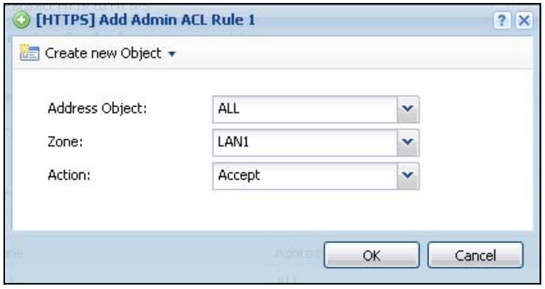
☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
-	ALL	ALL	accept

3 In the **Zone** field select **LAN1** and click **OK**.

Figure 96 Configuration > System > WWW > Service Control Rule Edit


[HTTPS] Add Admin ACL Rule 1
Create new Object
OK
Cancel

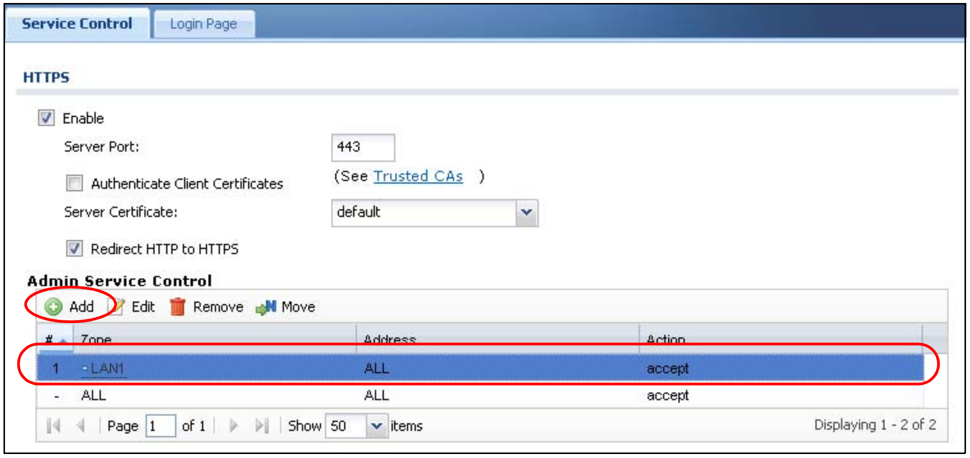
Address Object: ALL

Zone: LAN1

Action: Accept

4 Select the new rule and click the **Add** icon.

Figure 97 Configuration > System > WWW (First Example Admin Service Rule Configured)


Service Control
Login Page
Add
Edit
Remove
Move
Page 1 of 1
Show 50 items
Displaying 1 - 2 of 2

HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

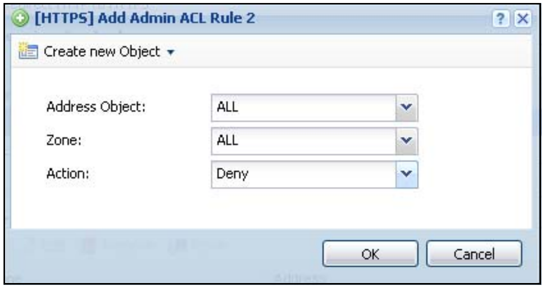
☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
1	LAN1	ALL	accept
-	ALL	ALL	accept

5 In the **Zone** field select **ALL** and set the **Action** to **Deny**. Click **OK**.

Figure 98 Configuration > System > WWW > Service Control Rule Edit



[HTTPS] Add Admin ACL Rule 2

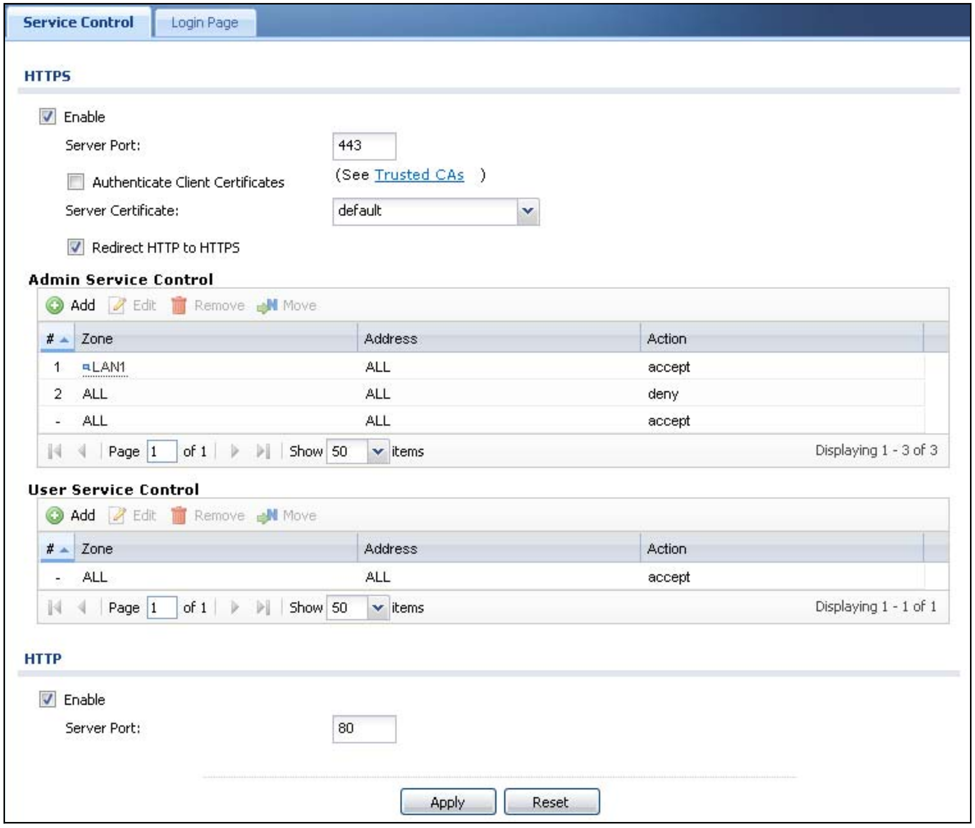
Address Object: ALL

Zone: ALL

Action: Deny

6 Click **Apply**.

Figure 99 Configuration > System > WWW (Second Example Admin Service Rule Configured)



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
1	LAN1	ALL	accept
2	ALL	ALL	deny
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

User Service Control

#	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

HTTP

☑ Enable

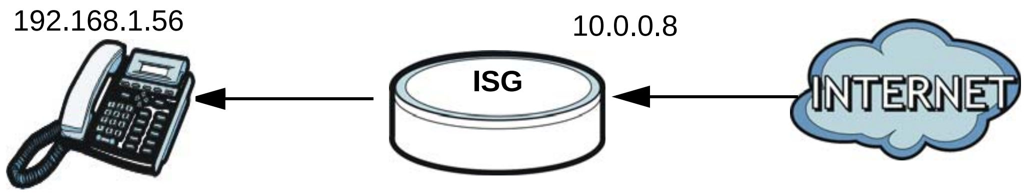
Server Port: 80

Now administrator access to the Web Configurator can only come from the LAN1 zone. Non-admin users can still use HTTPS to log into the ISG50 from any of the ISG50’s zones.

7.9 How to Allow Incoming H.323 Peer-to-peer Calls

Suppose you have a H.323 device on the LAN1 for VoIP calls and you want it to be able to receive peer-to-peer calls from the WAN. Here is an example of how to configure NAT and the firewall to have the ISG50 forward H.323 traffic destined for wan1 IP address 10.0.0.8 to a H.323 device located on the LAN and using IP address 192.168.1.56.

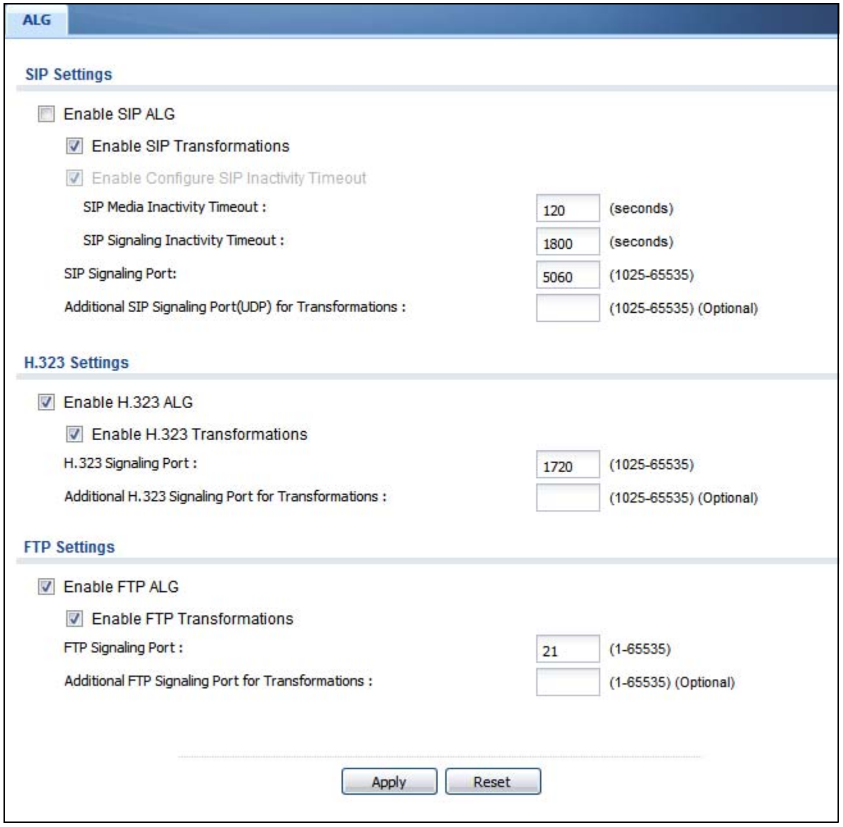
Figure 100 WAN to LAN H.323 Peer-to-peer Calls Example



7.9.1 Turn On the ALG

Click **Configuration > Network > ALG**. Select **Enable H.323 ALG** and **Enable H.323 transformations** and click **Apply**.

Figure 101 Configuration > Network > ALG



SIP Settings

☐ Enable SIP ALG
☑ Enable SIP Transformations
☑ Enable Configure SIP Inactivity Timeout
SIP Media Inactivity Timeout : 120 (seconds)
SIP Signaling Inactivity Timeout : 1800 (seconds)
SIP Signaling Port: 5060 (1025-65535)
Additional SIP Signaling Port(UDP) for Transformations : (1025-65535) (Optional)

H.323 Settings

☑ Enable H.323 ALG
☑ Enable H.323 Transformations
H.323 Signaling Port : 1720 (1025-65535)
Additional H.323 Signaling Port for Transformations : (1025-65535) (Optional)

FTP Settings

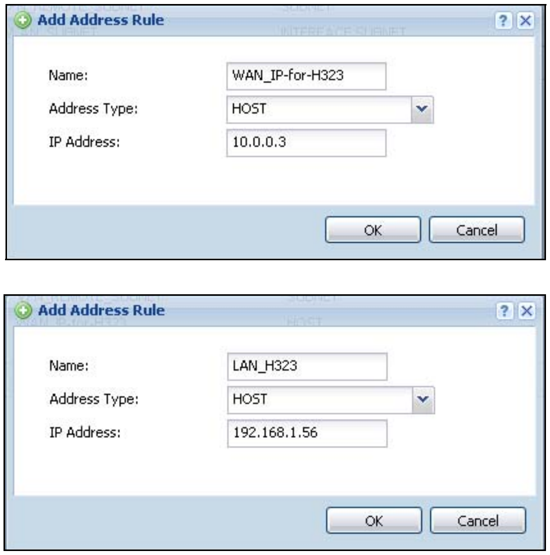
☑ Enable FTP ALG
☑ Enable FTP Transformations
FTP Signaling Port : 21 (1-65535)
Additional FTP Signaling Port for Transformations : (1-65535) (Optional)

7.9.2 Set Up a NAT Policy For H.323

In this example, you need a NAT policy to forward H.323 (TCP port 1720) traffic received on the ISG50's 10.0.0.8 WAN IP address to LAN1 IP address 192.168.1.56.

1 Use **Configuration > Object > Address > Add** to create an address object for the public WAN IP address (called WAN_IP-for-H323 here). Then use it again to create an address object for the H.323 device's private LAN1 IP address (called LAN_H323 here).

Figure 102 Create Address Objects



Name: WAN_IP-for-H323
Address Type: HOST
IP Address: 10.0.0.3

Name: LAN_H323
Address Type: HOST
IP Address: 192.168.1.56

2 Click **Configuration > Network > NAT > Add.**

Configure a name for the rule (WAN-LAN_H323 here).

You want the LAN H.323 device to receive peer-to-peer calls from the WAN and also be able to initiate calls to the WAN so you set the **Classification** to **NAT 1:1**.

Set the **Incoming Interface** to **wan1**.

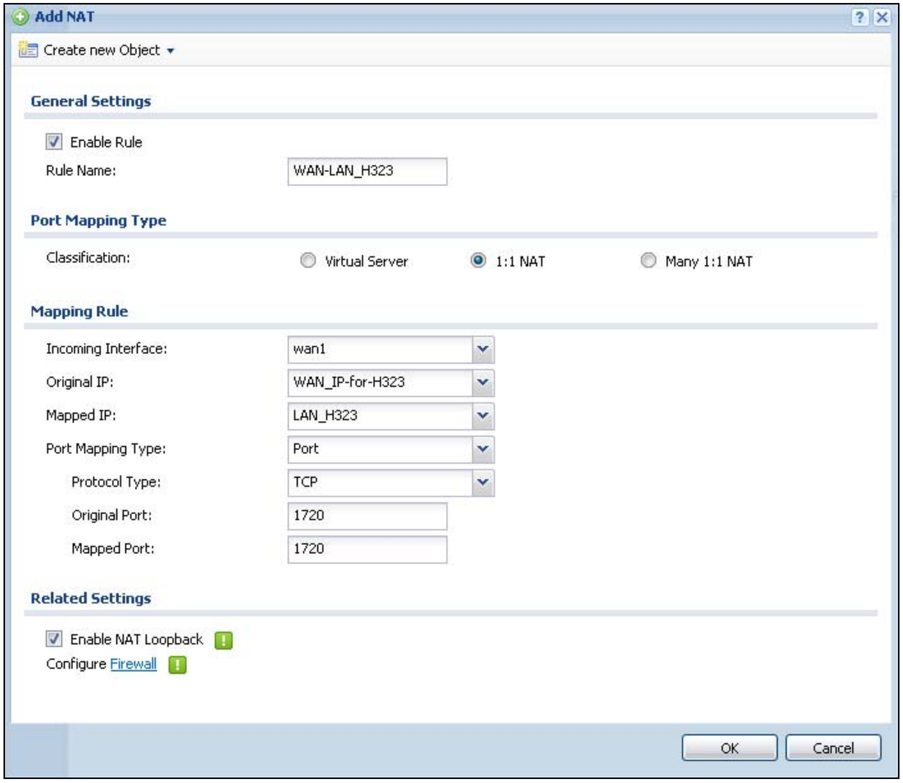
Set the **Original IP** to the WAN address object (**WAN_IP-for-H323**).

Set the **Mapped IP** to the H.323 device's LAN1 IP address object (**LAN_H323**).

Set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP** and the original and mapped ports to 1720.

Click **OK**.

Figure 103 Configuration > Network > NAT > Add



General Settings

☑ Enable Rule

Rule Name: WAN-LAN_H323

Port Mapping Type

Classification: ○ Virtual Server ● 1:1 NAT ○ Many 1:1 NAT

Mapping Rule

Incoming Interface: wan1

Original IP: WAN_IP-for-H323

Mapped IP: LAN_H323

Port Mapping Type: Port

Protocol Type: TCP

Original Port: 1720

Mapped Port: 1720

Related Settings

☑ Enable NAT Loopback

Configure Firewall

7.9.3 Set Up a Firewall Rule For H.323

The default firewall rule for WAN-to-LAN traffic drops all traffic. Here is how to configure a firewall rule to allow H.323 (TCP port 1720) traffic received on the WAN_IP-for-H323 IP address to go to LAN1 IP address 192.168.1.56.

1 Click **Configuration > Firewall** > **Add**.

In the **From** field select WAN.

In the **To** field select LAN1.

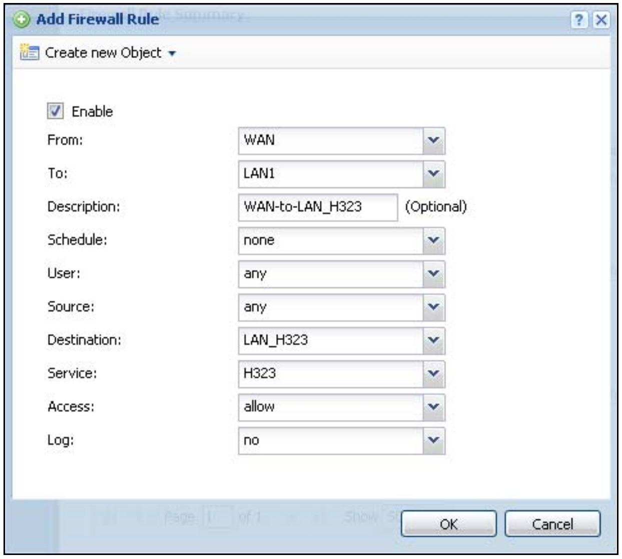
Configure a name for the rule (WAN-to-LAN_H323 here).

Set the **Destination** to the H.323 device's LAN1 IP address object (**LAN_H323**). **LAN_H323** is the destination because the ISG50 applies NAT to traffic before applying the firewall rule.

Set the **Service** to **H.323**.

Click **OK**.

Figure 104 Configuration > Firewall > Add



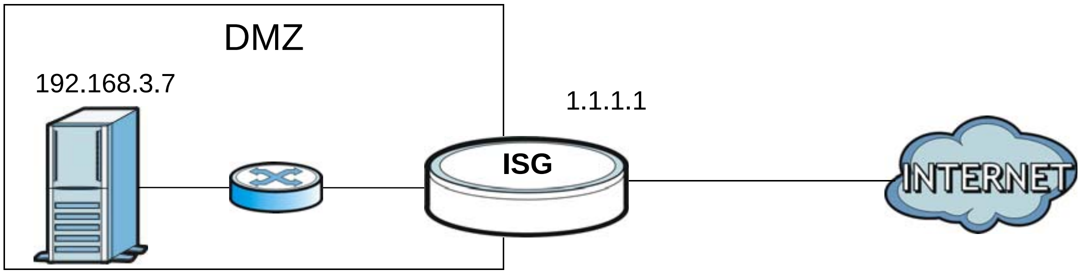
☑ Enable

From:	WAN
To:	LAN1
Description:	WAN-to-LAN_H323 (Optional)
Schedule:	none
User:	any
Source:	any
Destination:	LAN_H323
Service:	H323
Access:	allow
Log:	no

7.10 How to Allow Public Access to a Web Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). In this example you have public IP address 1.1.1.1 that you will use on the **wan1** interface and map to the HTTP server's private IP address of 192.168.3.7.

Figure 105 Public Server Example Network Topology

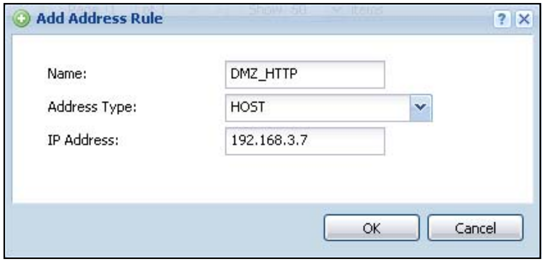


7.10.1 Create the Address Objects

Use **Configuration > Object > Address > Add** to create the address objects.

1 Create a host address object named DMZ_HTTP for the HTTP server's private IP address of 192.168.3.7.

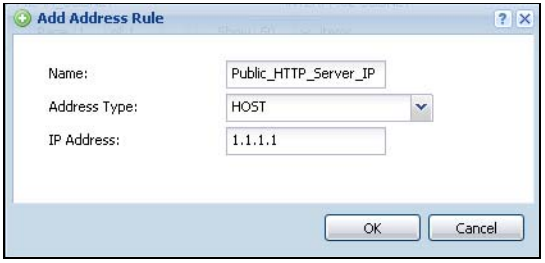
Figure 106 Creating the Address Object for the HTTP Server's Private IP Address



Name: DMZ_HTTP
Address Type: HOST
IP Address: 192.168.3.7

2 Create a host address object named Public_HTTP_Server_IP for the public WAN IP address 1.1.1.1.

Figure 107 Creating the Address Object for the Public IP Address



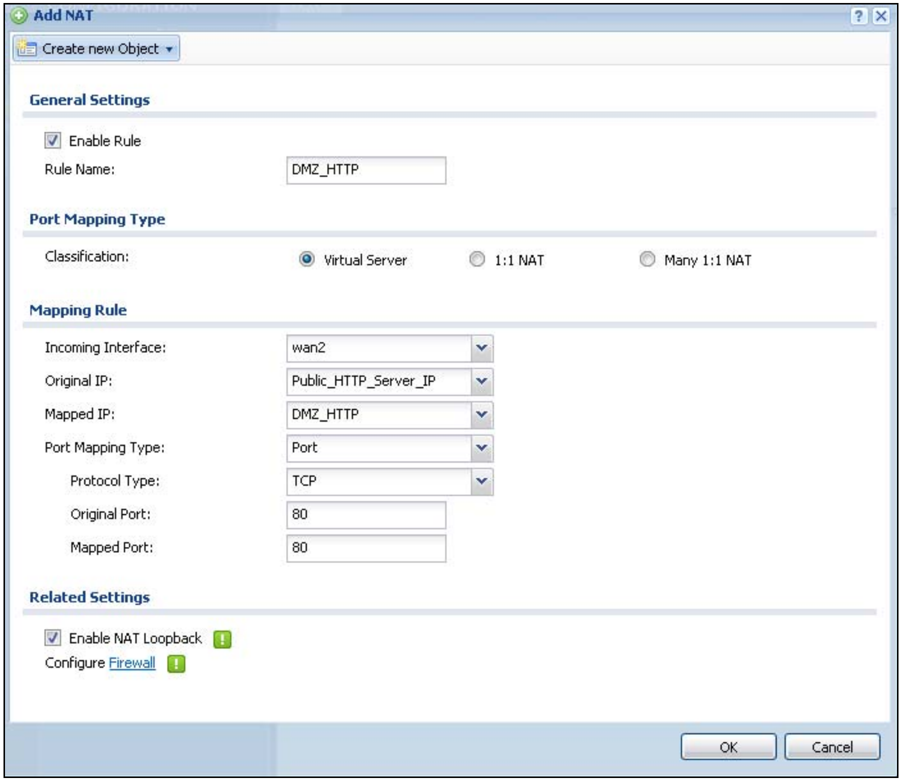
Name: Public_HTTP_Server_IP
Address Type: HOST
IP Address: 1.1.1.1

7.10.2 Configure NAT

You need a NAT rule to send HTTP traffic coming to IP address 1.1.1.1 on **wan1** to the HTTP server's private IP address of 192.168.3.7. In the **Configuration > Network > NAT** screen, click the **Add** icon and create a new NAT entry as follows.

- Set the **Incoming Interface** to **wan1**.
- Set the **Original IP** to the **Public_HTTP_Server_IP** object and the **Mapped IP** to the **DMZ_HTTP** object.
- HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP**, and the original and mapped ports to 80.
- Keep **Enable NAT Loopback** selected to allow users connected to other interfaces to access the HTTP server (see NAT Loopback on page 328 for details).

Figure 108 Creating the NAT Entry



General Settings

☑ Enable Rule

Rule Name: DMZ_HTTP

Port Mapping Type

Classification: ● Virtual Server ○ 1:1 NAT ○ Many 1:1 NAT

Mapping Rule

Incoming Interface: wan2

Original IP: Public_HTTP_Server_IP

Mapped IP: DMZ_HTTP

Port Mapping Type: Port

Protocol Type: TCP

Original Port: 80

Mapped Port: 80

Related Settings

☑ Enable NAT Loopback

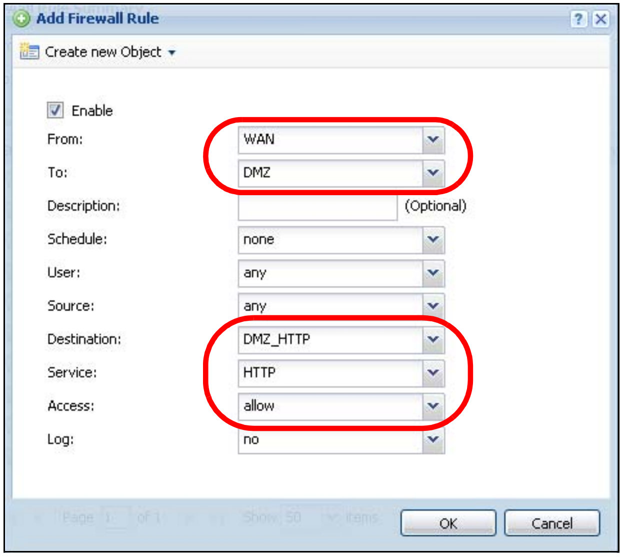
Configure Firewall

7.10.3 Set Up a Firewall Rule

The firewall blocks traffic from the WAN zone to the DMZ zone by default so you need to create a firewall rule to allow the public to send HTTP traffic to IP address 1.1.1.1 in order to access the HTTP server. If a domain name is registered for IP address 1.1.1.1, users can just go to the domain name to access the web server.

1 Click **Configuration > Firewall** > **Add**. Set the **From** field as **WAN** and the **To** field as **DMZ**. Set the **Destination** to the HTTP server's DMZ IP address object (**DMZ_HTTP**). **DMZ_HTTP** is the destination because the ISG50 applies NAT to traffic before applying the firewall rule. Set the **Access** field to **allow** and the **Service** to **HTTP**, and click **OK**.

Figure 109 Configuration > Firewall > Add



☑ Enable

From: WAN

To: DMZ

Description: (Optional)

Schedule: none

User: any

Source: any

Destination: DMZ_HTTP

Service: HTTP

Access: allow

Log: no

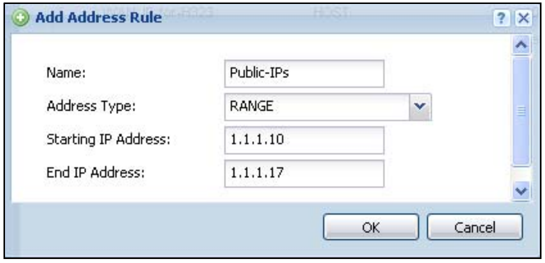
7.11 How to Use Multiple Static Public WAN IP Addresses for LAN to WAN Traffic

If your ISP gave you a range of static public IP addresses, here is how to configure a policy route to have the ISG50 use them for traffic it sends out from the LAN.

7.11.1 Create the Public IP Address Range Object

Click **Configuration > Object > Address > Add** to create the address object that represents the range of static public IP addresses. In this example you name it Public-IPs and it goes from 1.1.1.10 to 1.1.1.17.

Figure 110 Creating the Public IP Address Range Object



Name: Public-IPs

Address Type: RANGE

Starting IP Address: 1.1.1.10

End IP Address: 1.1.1.17

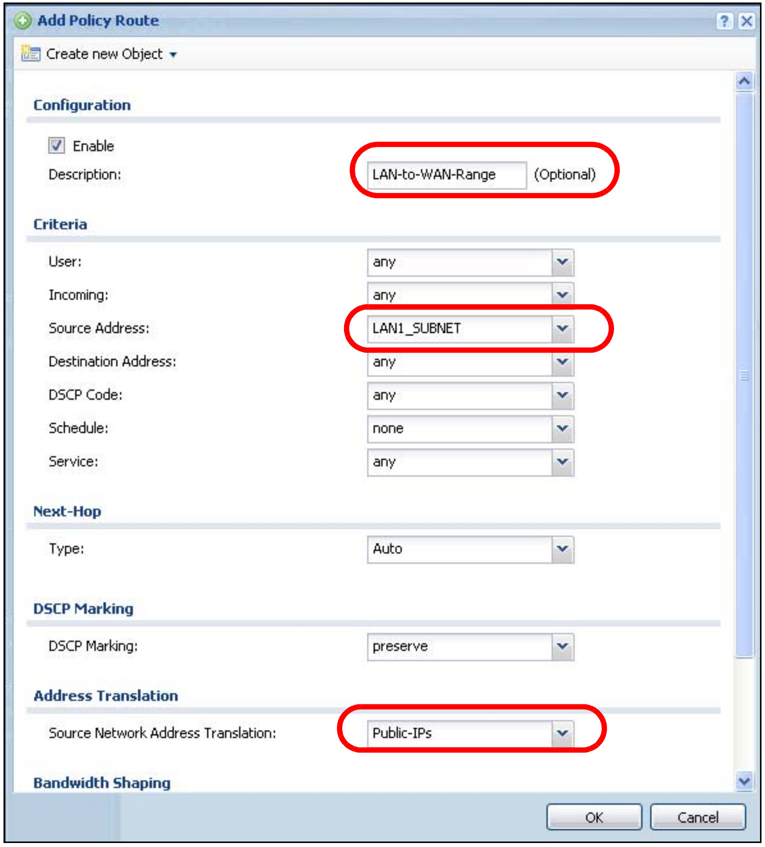
7.11.2 Configure the Policy Route

Now you need to configure a policy route that has the ISG50 use the range of public IP addresses as the source address for WAN to LAN traffic.

Click **Configuration > Network > Routing > Add**.

Although adding a description is optional, it is recommended. This example uses LAN-to-WAN-Range. Specifying a **Source Address** is also optional although recommended. This example uses **LAN_SUBNET1**. Set the **Source Network Address Translation** to **Public-IPs** and click **OK**.

Figure 111 Configuring the Policy Route



Configuration

☑ Enable

Description: LAN-to-WAN-Range (Optional)

Criteria

User: any

Incoming: any

Source Address: LAN1_SUBNET

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

Next-Hop

Type: Auto

DSCP Marking

DSCP Marking: preserve

Address Translation

Source Network Address Translation: Public-IPs

Bandwidth Shaping

7.12 Initial Setup Video

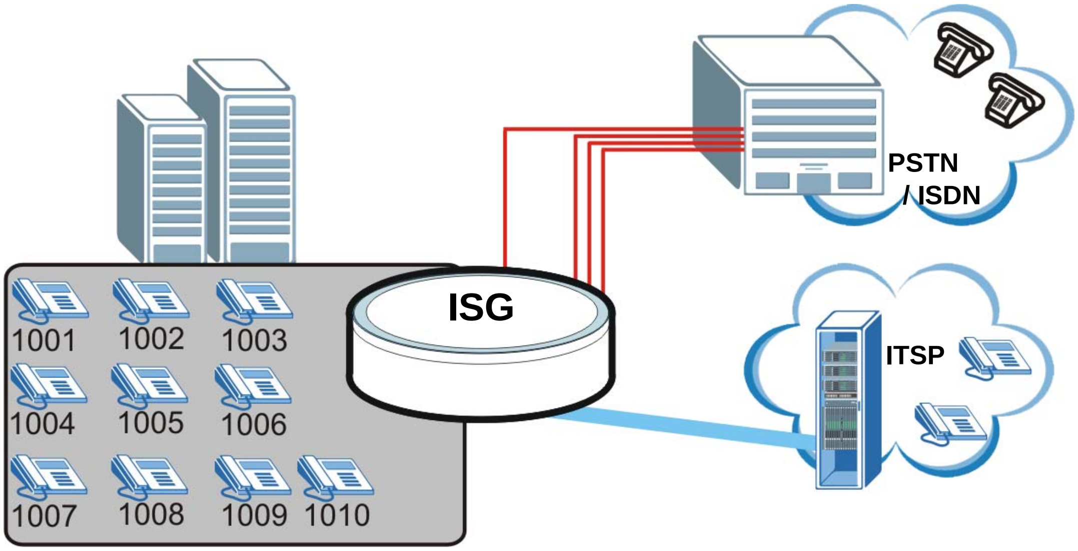
Use Adobe Reader 9 or later or a recent version of Foxit Reader to play this video. After clicking play, you may need to confirm that you want to play the content and click play again.

8

PBX Tutorials

Here are examples of using the web configurator to set up and use the ISG50 for a telephone network as shown in the following figure.

Figure 112 Tutorial Overview



The tutorials include:

Table 19 Tutorials Overview

TUTORIAL GOAL	STEPS
Making Internal Calls	• Configure SIP Extensions • Connect IP Phones • Register IP Phones
Auto Provisioning	• Configuring the snom VoIP Phones for Auto Provisioning
Making PSTN Calls	• The PSTN Connection • Creating a Dialing Rule for PSTN • Assigning an LCR to an Authority Group
Making ITSP Calls	• The ITSP Connection • Creating a Dialing Rule for ITSP • Assigning an LCR to an Authority Group
Making ISDN Calls	• The ISDN Connection • Creating a Dialing Rule for ISDN • Assigning an LCR to an Authority Group
ISDN Network Configuration Examples	• Example 1: Small/Medium Business • Example 2: Company with Existing PBX • Example 3: Company with Existing PBX and Expanding Employees

Table 19 Tutorials Overview

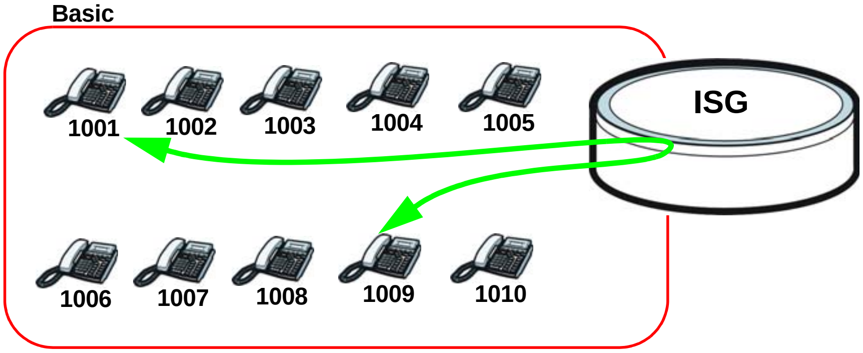
TUTORIAL GOAL	STEPS
Using Call Features	• Customizing Feature Codes • Using the Voicemail Feature
Using the Extension Portal	• Your Information • Accessing the Extension Portal • Changing Your Security Information • Personalizing Your Settings • Setting Up Voicemail
Capturing Packets Using the Web Configurator	• Capturing Packets Using the Web Configurator
Creating an Automated Menu System	• Create an Agent Identity • Create a Skill • Create an Auto-Attendant

Note: This chapter assumes that you have already configured your network settings. See the QSG, the installation wizard Chapter 4 on page 59, Chapter 5 on page 69, and Chapter 7 on page 107 for more information.

8.1 Making Internal Calls

This tutorial sets up the internal telephone extensions on your network. At the end of this tutorial you should be able to call between extensions. The next figure shows the telephone extensions **1001** - **1010** are configured in this tutorial. All of the extensions are members of an authority group called **Basic** (you create an authority group and then add extensions). The figure also shows an internal call between extensions **1001** and **1009**.

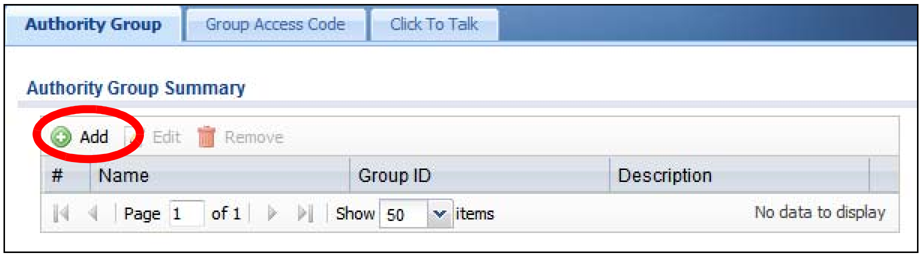
Figure 113 Internal Calls



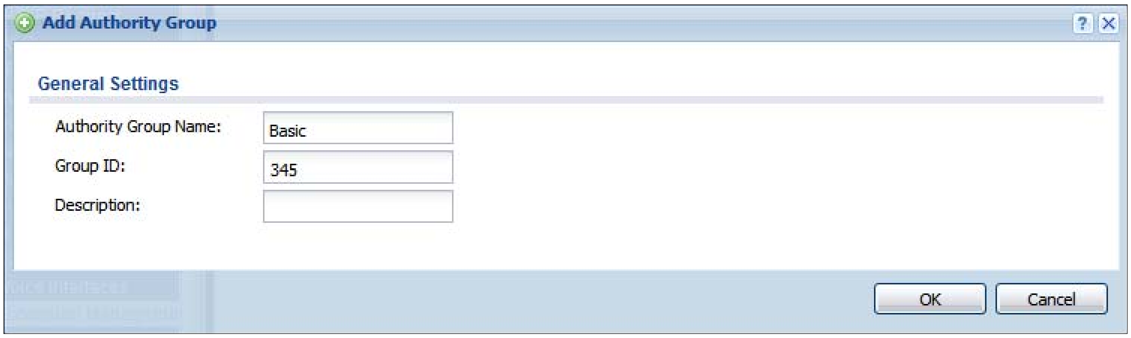
8.1.1 Configure SIP Extensions

The following section introduces how to create the authority group called **Basic** and ten SIP extensions **1001** to **1010** on the ISG50. The number of extensions you can create is limited by your service subscription (see Chapter 11 on page 229).

1 In the web configurator, click **Configuration > PBX > Extension Management > Authority Group** to open the **Authority Group** screen.

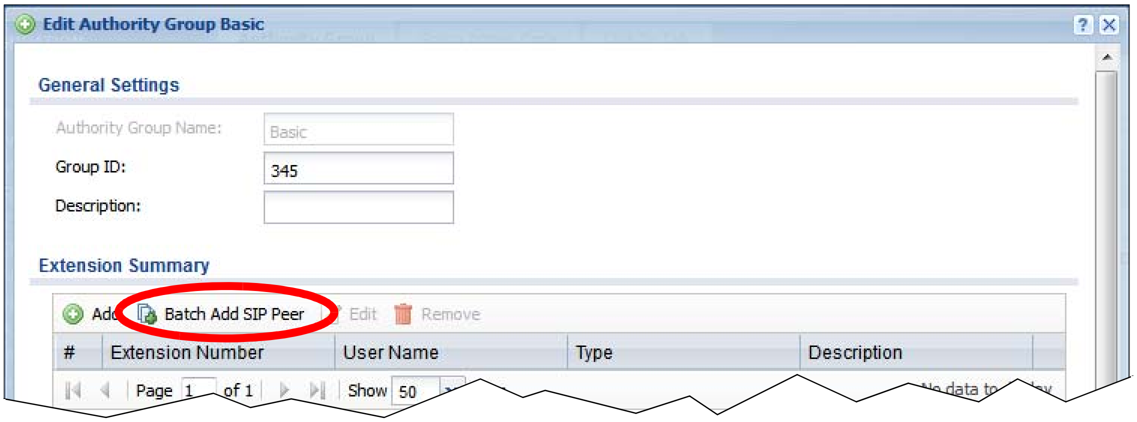

Authority Group
Group Access Code
Click To Talk
Authority Group Summary
Add
Edit
Remove
#
Name
Group ID
Description
Page 1 of 1
Show 50 items
No data to display

2 Click the **Add** icon to open the **Add** screen. Enter the name of the group (**Basic** in this example) and type 1-5 digits to use as an ID for this authority group (**345** here). Click **OK**.


Add Authority Group
General Settings
OK
Cancel

Authority Group Name: Basic
Group ID: 345
Description:

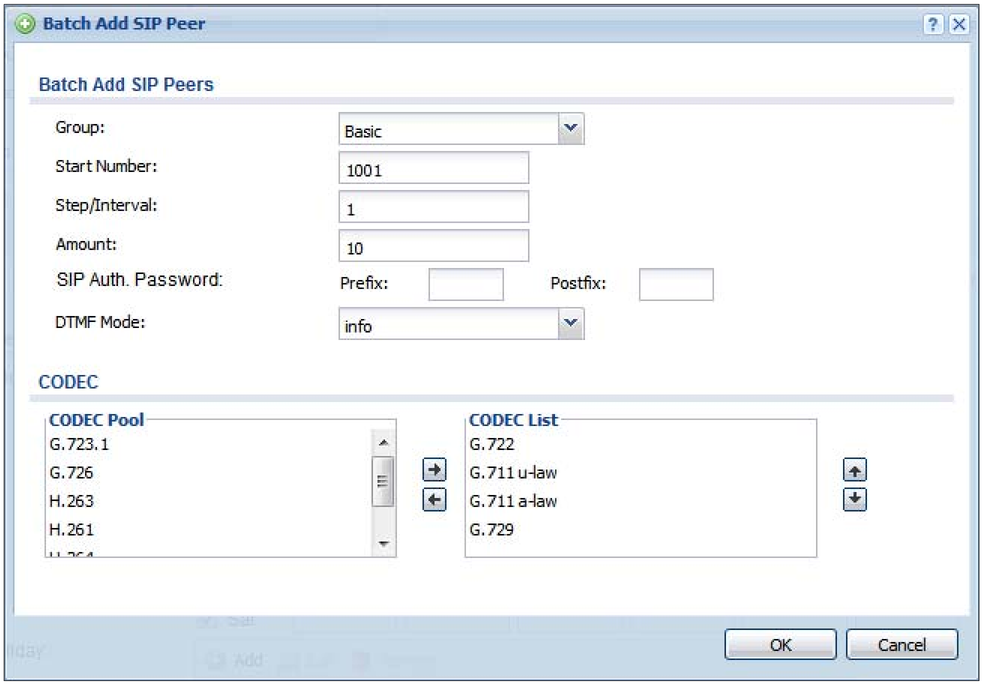
3 The **Edit Authority Group Basic** screen displays. Click **Batch Add SIP Peer** to configure multiple SIP accounts at the same time.


Edit Authority Group Basic
General Settings
Extension Summary
Add
Batch Add SIP Peer
Edit
Remove
#
Extension Number
User Name
Type
Description
Page 1 of 1
Show 50

Authority Group Name: Basic
Group ID: 345
Description:

4 The **Batch Add SIP Peer** screen opens. The SIP extension number and any configured **SIP Auth. Password** prefix and/or postfix make up the SIP password. The SIP password must be at least four digits. This example uses ten four-digit SIP extensions **1001** - **1010** that are also used as the SIP usernames. The SIP passwords are comprised of the combination of **Prefix** + **Extension** + **Postfix**. In this example, the **SIP Auth. Password Prefix** value is **11** and the **Postfix** value is **99**.

The SIP username for extension **1001** is **1001** and the SIP password for this extension is **11100199**. You do not need to configure the **Prefix** and **Postfix** values as long as the SIP password length is at least four digits long. Click **OK** and wait for the ISG50 to create the extensions.



Batch Add SIP Peer

Batch Add SIP Peers

Group: Basic

Start Number: 1001

Step/Interval: 1

Amount: 10

SIP Auth. Password: Prefix: Postfix:

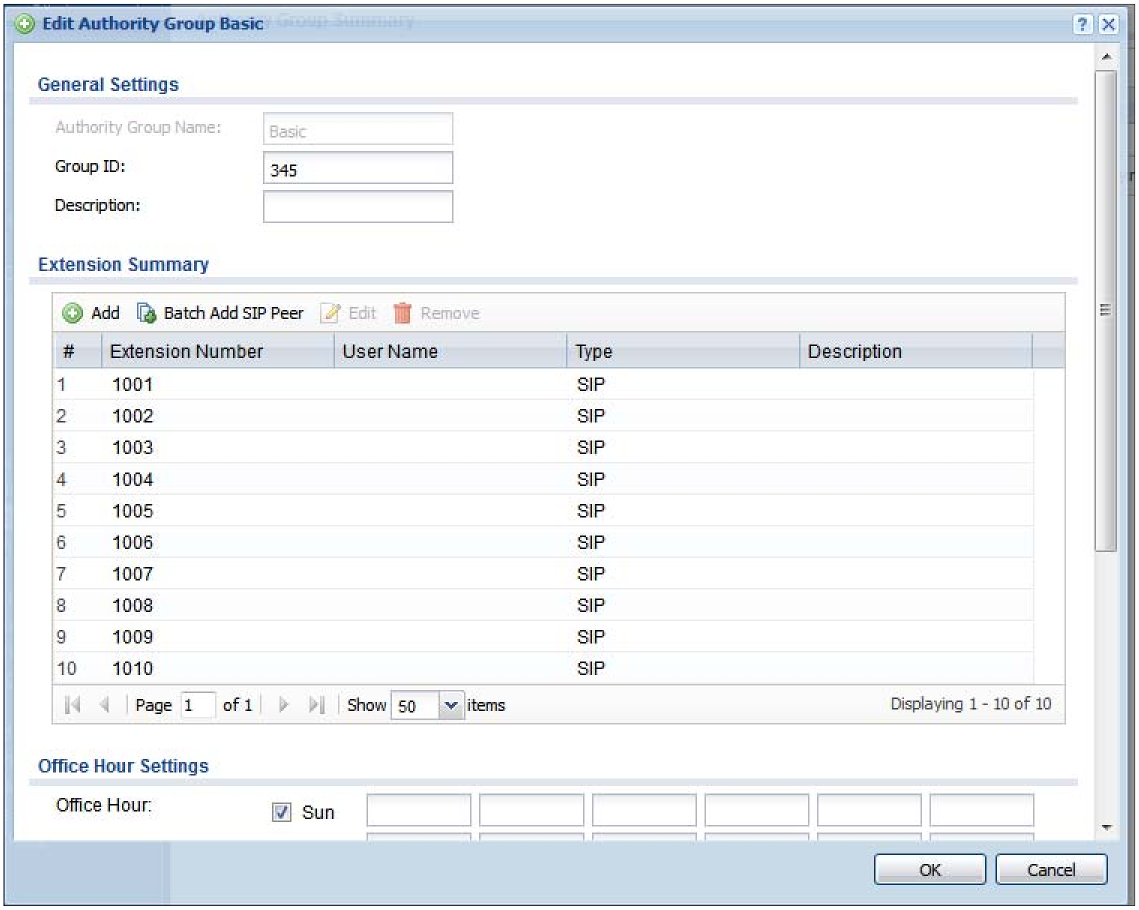
DTMF Mode: info

CODEC

CODEC Pool: G.723.1, G.726, H.263, H.261

CODEC List: G.722, G.711 u-law, G.711 a-law, G.729

5 The SIP extensions display in the **Edit Authority Group Basic** screen. Click **OK**.


Edit Authority Group Basic
General Settings
Extension Summary
Add
Batch Add SIP Peer
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 10 of 10
Office Hour Settings
OK
Cancel

Authority Group Name: Basic
Group ID: 345
Description:

#	Extension Number	User Name	Type	Description
1	1001		SIP	
2	1002		SIP	
3	1003		SIP	
4	1004		SIP	
5	1005		SIP	
6	1006		SIP	
7	1007		SIP	
8	1008		SIP	
9	1009		SIP	
10	1010		SIP	

Office Hour: ☑ Sun

6 Keep a list of the SIP passwords (the **Prefix** + **Extension Number** + **Postfix** combinations). When you deploy the network's IP phones, you will need this information for SIP registration. See Section 8.1.2 on page 140 for information on configuring your IP phones.

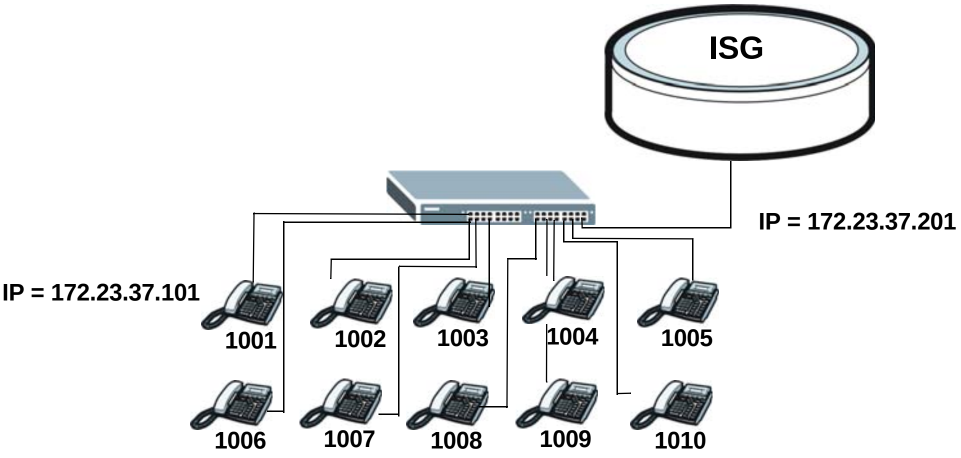
The extension number serves as the password the user uses to log into the ISG50 to configure his extension's call forwarding, call blocking, phonebook, voice mail, and other settings. See Chapter 60 on page 757 for more information.

7 If the IP phone is a snom or snom-compatible SIP client, use Section 8.2 on page 141 to map the SIP extensions to your network's SIP devices.

8.1.2 Connect IP Phones

You can now set up your IP phones. For example, you can connect all of the IP phones and the ISG50 to an Ethernet switch and assign all the IP phones IP addresses in the same subnet.

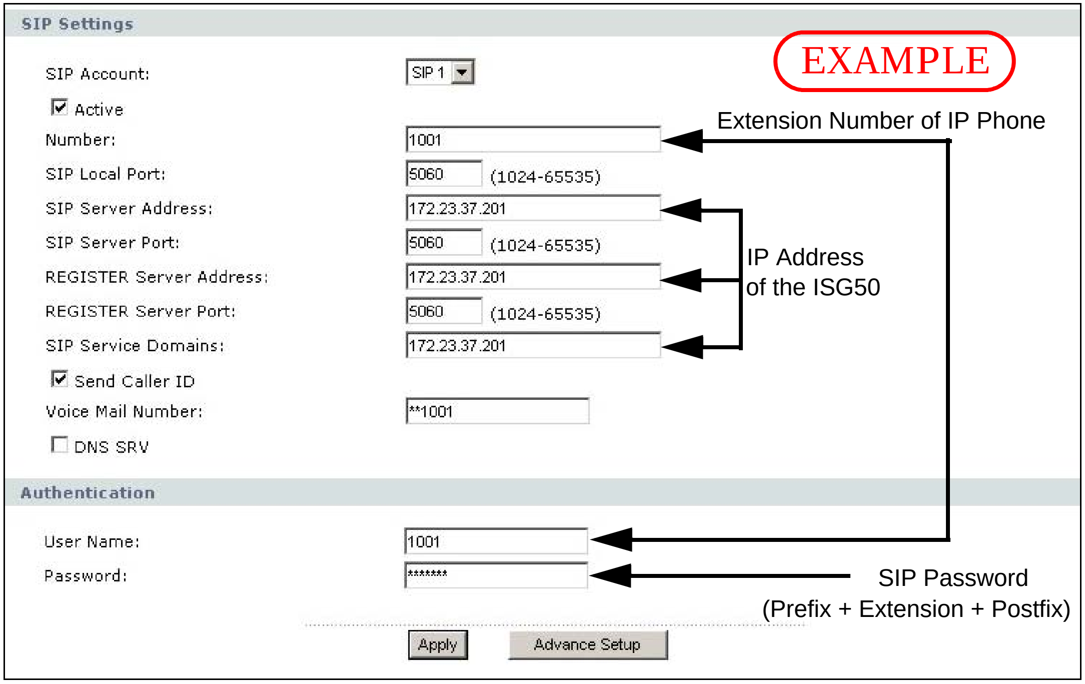
Figure 114 Connect IP Phones



8.1.3 Register IP Phones

After your network connections have been made, you can proceed with the SIP registration of the IP phones on your network. The next figure shows a typical SIP registration screen of a ZyXEL IP phone. This is a sample screen only, but it includes all the key fields necessary to complete a SIP registration. It shows the SIP registration of an IP phone with the extension **1001**.

Figure 115 Example IP Phone SIP Registration Screen



SIP Settings

SIP Account: SIP 1
☑ Active
Number: 1001
SIP Local Port: 5060 (1024-65535)
SIP Server Address: 172.23.37.201
SIP Server Port: 5060 (1024-65535)
REGISTER Server Address: 172.23.37.201
REGISTER Server Port: 5060 (1024-65535)
SIP Service Domains: 172.23.37.201
☑ Send Caller ID
Voice Mail Number: **1001
☐ DNS SRV

Authentication

User Name: 1001
Password: *******

EXAMPLE

Extension Number of IP Phone

IP Address of the ISG50

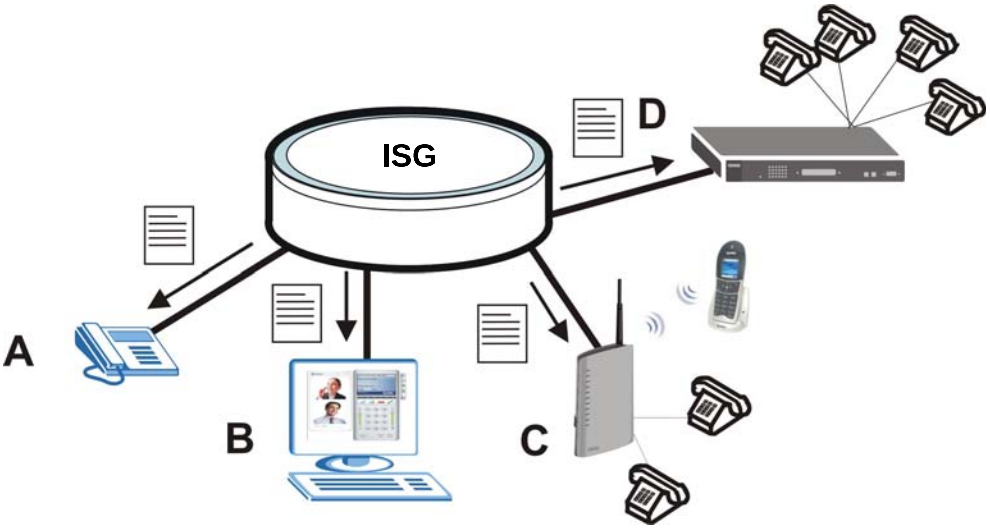
SIP Password (Prefix + Extension + Postfix)

Complete the SIP registration for all the IP phones on your network. When all the phones are registered, you can make internal calls by dialing the extension number assigned to each phone.

8.2 Auto Provisioning

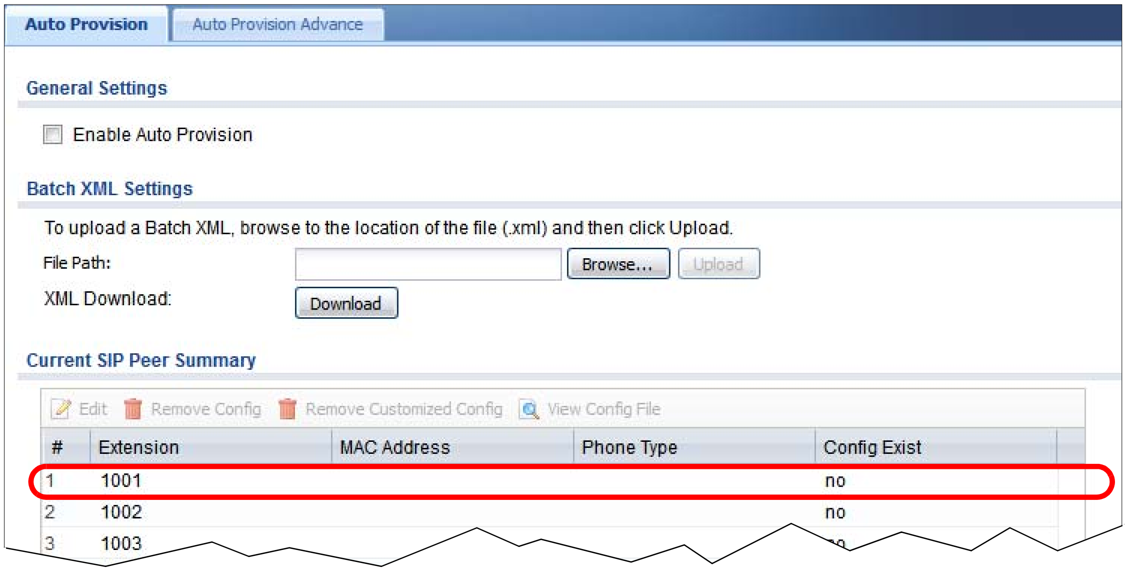
You can have snom VoIP phones get a configuration text file from the ISG50. The configuration file contains the SIP settings that the SIP device uses to register with the ISG50. The following graphic shows an IP phone (**A**), softphone (**B**), ATA (**C**), and VoIP gateway (**D**) downloading configuration text files from the ISG50.

Figure 116 Auto Provisioning



After you configure the SIP extensions (see Section 8.1.1 on page 136) and make your network connections (see Figure 114 on page 140), use the following directions to map each SIP extension to the appropriate snom device. You need the MAC address of each snom device.

1 Click **Configuration > PBX > Auto Provision**. Then double-click a SIP extension entry.


Auto Provision
Auto Provision Advance
Browse...
Upload
Download
Edit
Remove Config
Remove Customized Config
View Config File

General Settings

☐ Enable Auto Provision

Batch XML Settings

To upload a Batch XML, browse to the location of the file (.xml) and then click Upload.

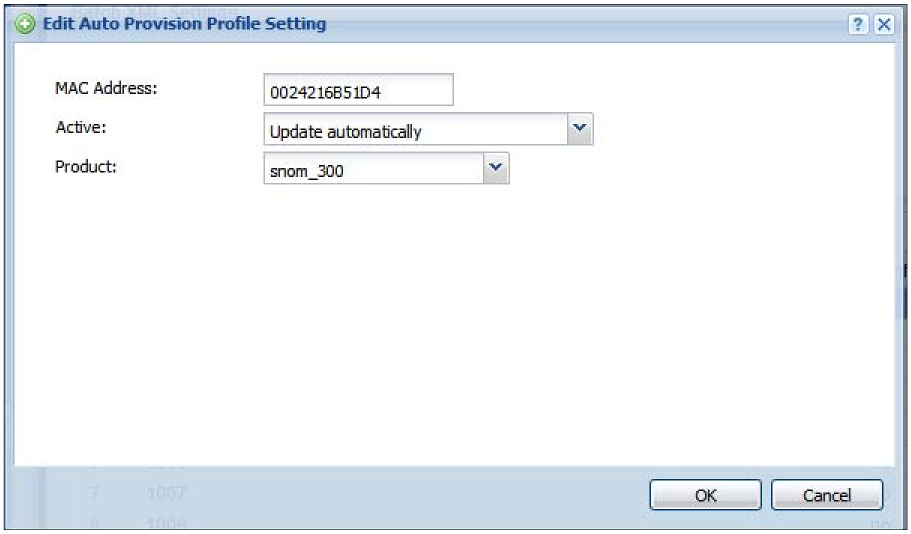
File Path:

XML Download:

Current SIP Peer Summary

#	Extension	MAC Address	Phone Type	Config Exist
1	1001			no
2	1002			no
3	1003			

2 Enter the SIP device's MAC address and select what model it is. Click **OK**.


Edit Auto Provision Profile Setting
OK
Cancel

MAC Address: 0024216B51D4

Active: Update automatically

Product: snom_300

3 Repeat these steps to map each SIP extension to a snom device's MAC.

8.2.1 Configuring the snom VoIP Phones for Auto Provisioning

Configure the snom phones to receive configuration information from the ISG50. This typically involves enabling auto provisioning through HTTP. See the snom phone's documentation for how to do this.

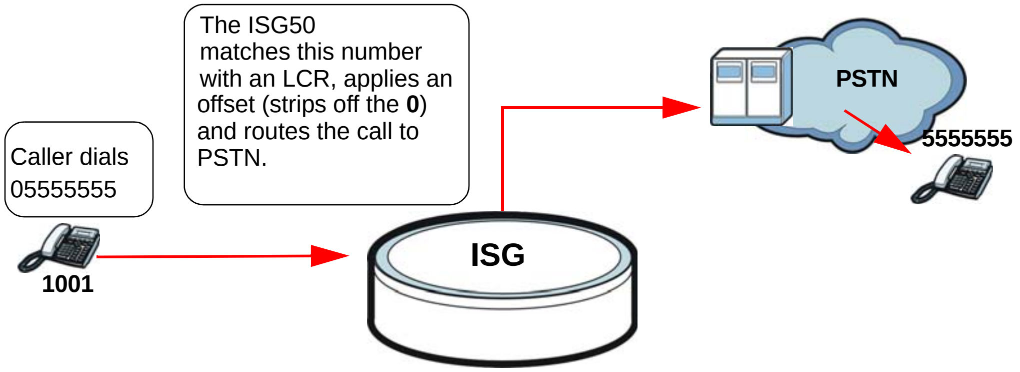
Once the snom phones receive their configuration information via auto provisioning, they will automatically register with the ISG50. You can make internal calls by dialing the extension number assigned to each phone.

8.3 Making PSTN Calls

The following section shows you how to make and receive calls via a connection to the PSTN. This example covers:

- The PSTN Connection - configuring the outbound line group (connection settings) from the FXO ports to the PSTN.
- Creating a Dialing Rule for PSTN - creating a rule which tells the ISG50 when to use the PSTN connection when completing outbound calls.
- Assigning an LCR to an Authority Group - giving extensions the right to make outbound calls via the PSTN connection.

Figure 117 Making a PSTN Call

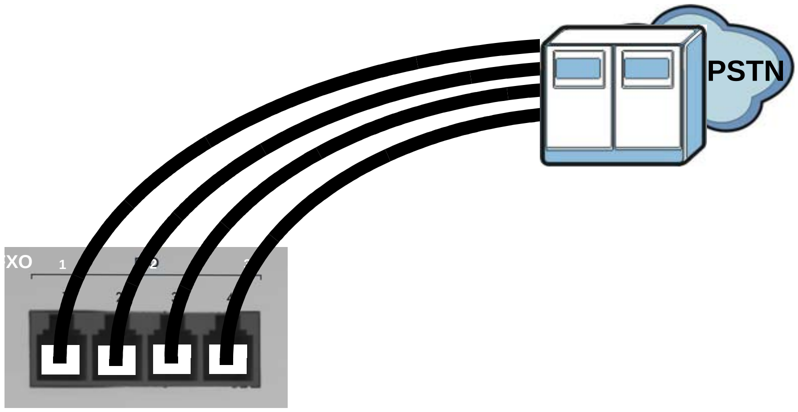

The ISG50 matches this number with an LCR, applies an offset (strips off the **0**) and routes the call to PSTN.
Caller dials 05555555
1001
ISG
PSTN
5555555

8.3.1 The PSTN Connection

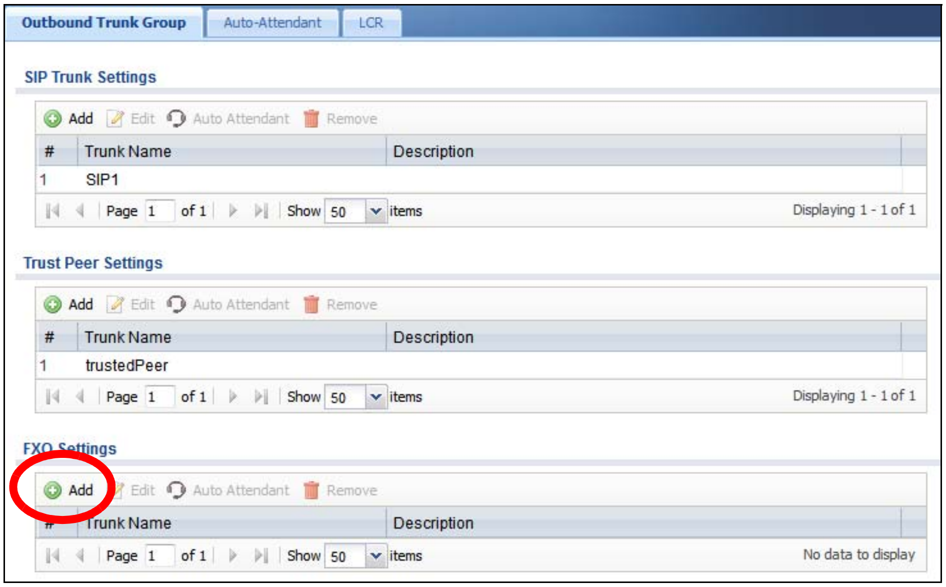
This example assumes that the ISG50 has an FXO interface already connected (refer to the Quick Start Guide) and that you have connected your telephone cables to the outlets that connect to your local telephone company. The front of your ISG50 should look as shown in the following figure.

In this example, ports **1**-**4** are used for the connections. You will use this information in a web configurator screen later.

Figure 118 FXO Connection



1 In the web configurator, click **Configuration > PBX > Outbound Line Management > Outbound Trunk Group** to open the **Outbound Trunk Group** screen.


Outbound Trunk Group
Auto-Attendant
LCR
SIP Trunk Settings
Add
Edit
Auto Attendant
Remove
Trust Peer Settings
FXO Settings
Page 1 of 1
Show 50 items

#	Trunk Name	Description
1	SIP1	

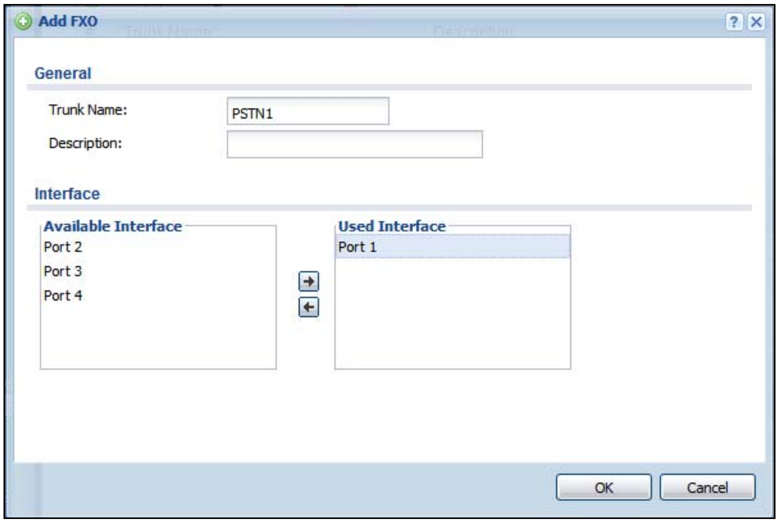
Displaying 1 - 1 of 1

#	Trunk Name	Description
1	trustedPeer	

Displaying 1 - 1 of 1

No data to display

2 In the **FXO Settings** section click the **Add** icon to open the following screen. Enter the name of the group (**PSTN1** in this example) and select the FXO ports that are to be members. Click **OK**.


Add FXO
General
Interface
Available Interface
Port 2
Port 3
Port 4
Used Interface
Port 1
OK
Cancel

Trunk Name: PSTN1

Description:

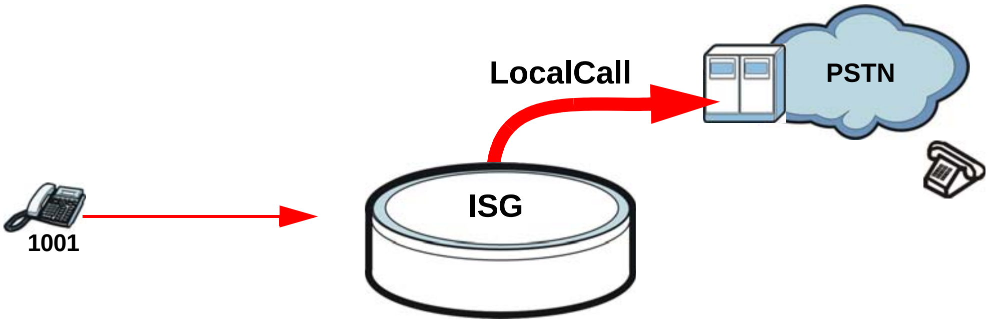
3 People from the outside world can now call the ISG50 using the PSTN numbers provided by your local telephone company. The default AA prompts the callers to dial the extension they would like to reach. See Section 8.3.2 on page 144 for information on how to set up a dialing rule so that the extensions on your network can connect to the PSTN.

8.3.2 Creating a Dialing Rule for PSTN

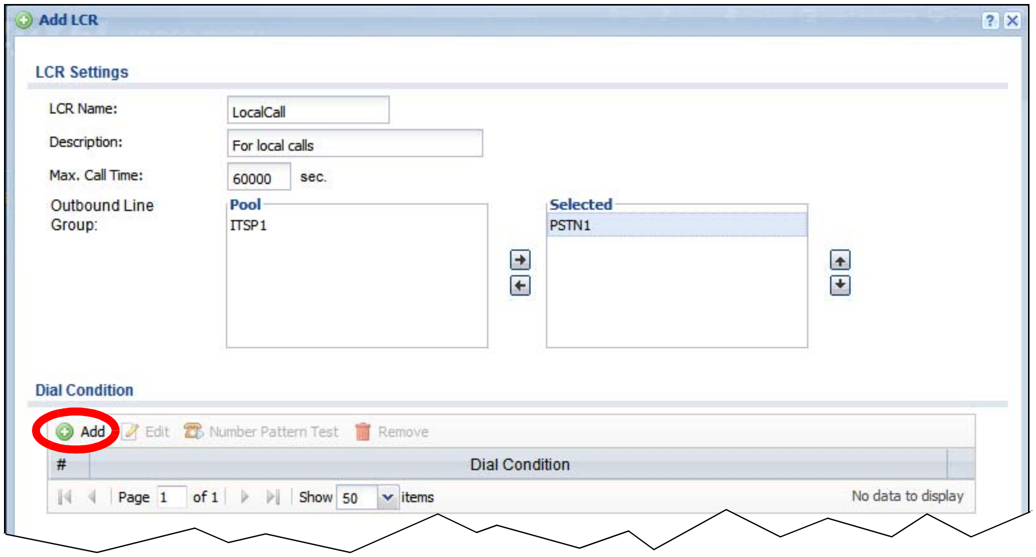
The following sections show you how to create outbound dialing rules (also referred to as Least Cost Routing or LCR).

The LCRs determine which outside line the ISG50 should use to complete outbound calls. In our example we want to use the **PSTN1** outbound line group to complete local calls.

Figure 119 Outbound Calls via PSTN



1 In the web configurator, click **Configuration > PBX > Outbound Line Management > LCR > Add** to open the **Add LCR** screen. Enter a name and description for the LCR. Move the outbound line group from the pool column that you want to add to this LCR (**PSTN1** in this example) to the **Selected** column. Then click the **Add** icon to configure a dial condition.



LCR Settings

LCR Name: LocalCall

Description: For local calls

Max. Call Time: 60000 sec.

Outbound Line Group: Pool: ITSP1; Selected: PSTN1

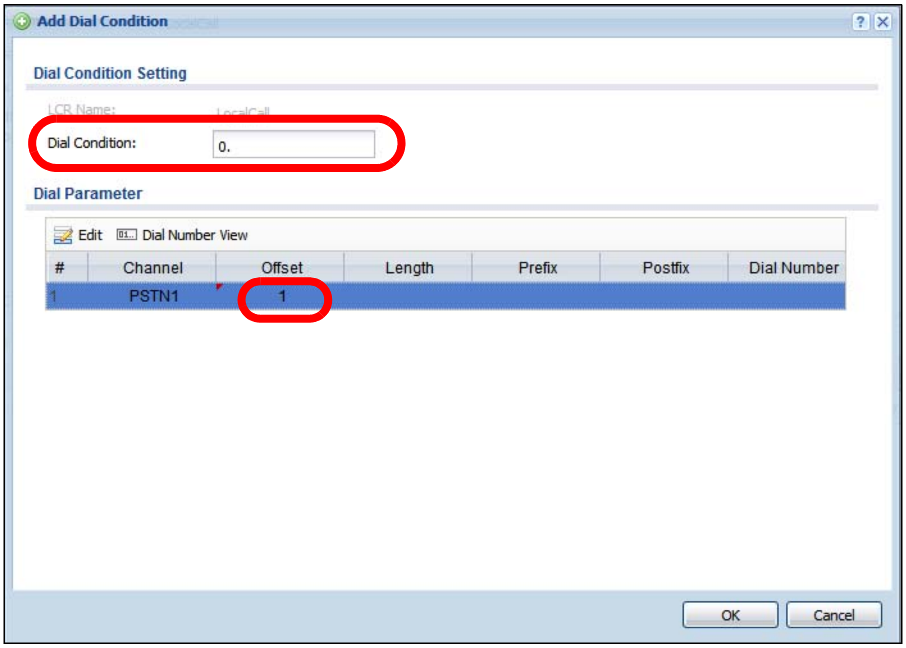
Dial Condition

#	Dial Condition

2 The **Dial Condition** screen appears.

- Type **0** followed by a period (**.**) in the **Dial Condition** field. This means that this LCR will be used when callers dial any number that begins with a **0**. The period (**.**) is a wildcard character, meaning anything can follow the zero.
- Specify an offset value. In our example, we configure an offset value of **1**. The offset value tells the ISG50 how many initial digits (if any) it should strip off of the dialed number before routing the call to the external line. See page 147 for an example.

- Click **OK**.


Add Dial Condition
Dial Condition Setting
Dial Parameter
Edit
Dial Number View
OK
Cancel

LCR Name: LocalCall

Dial Condition: 0.

#	Channel	Offset	Length	Prefix	Postfix	Dial Number
1	PSTN1	1				

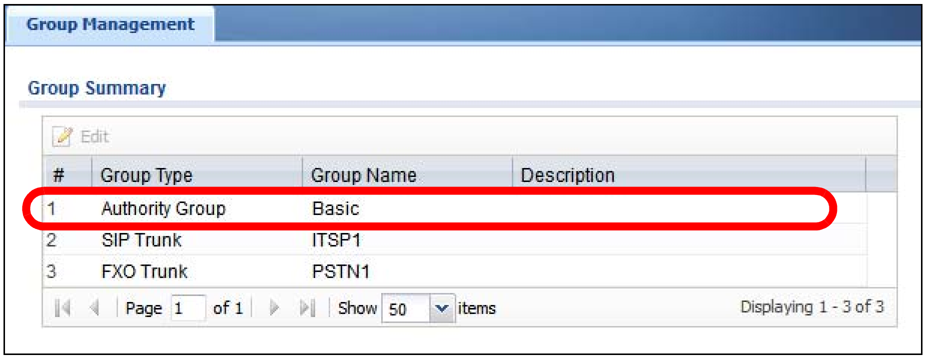
3 Click **OK** again and you are done configuring the LCR. However, before it can be used by any of the phones connected to the ISG50, the LCR needs to be assigned to an appropriate authority group.

8.3.3 Assigning an LCR to an Authority Group

Now add the LCR to an authority group to give the extensions in that group the right to use an LCR (outbound dial condition). In our example, we give the authority group **Basic** the right to call out using the LCR **LocalCall**.

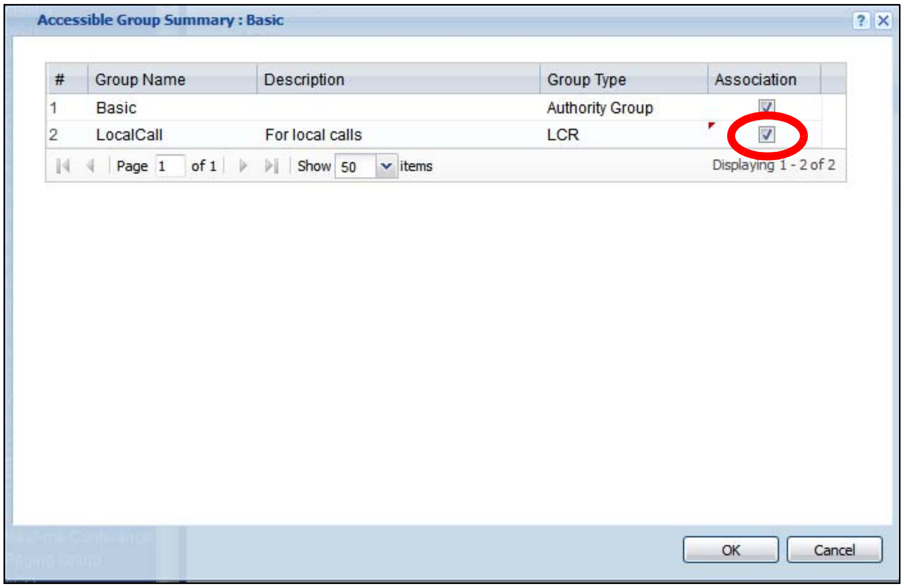
Procedure:

1 Click **Configuration** > **PBX** > **Group Management** and double-click the **Basic** entry.


Group Management
Group Summary
Edit
Page 1 of 1
Show 50 items
Displaying 1 - 3 of 3

#	Group Type	Group Name	Description
1	Authority Group	Basic	
2	SIP Trunk	ITSP1	
3	FXO Trunk	PSTN1	

2 Select the **LocalCall** entry's **Association** checkbox. Click **OK**.

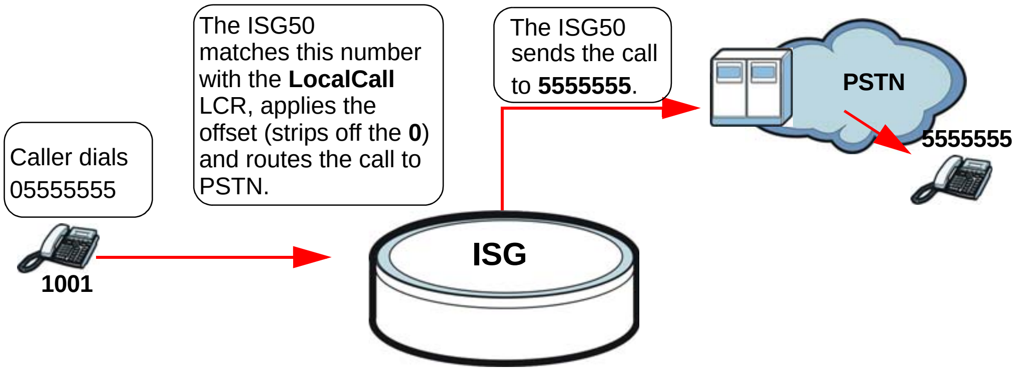


Accessible Group Summary : Basic

#	Group Name	Description	Group Type	Association
1	Basic		Authority Group	☑
2	LocalCall	For local calls	LCR	☑

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

3 You can now use the telephones that are part of the **FXOTrunk** authority group to make outbound calls using the PSTN connection. The following figure summarizes the outbound call process for this example.

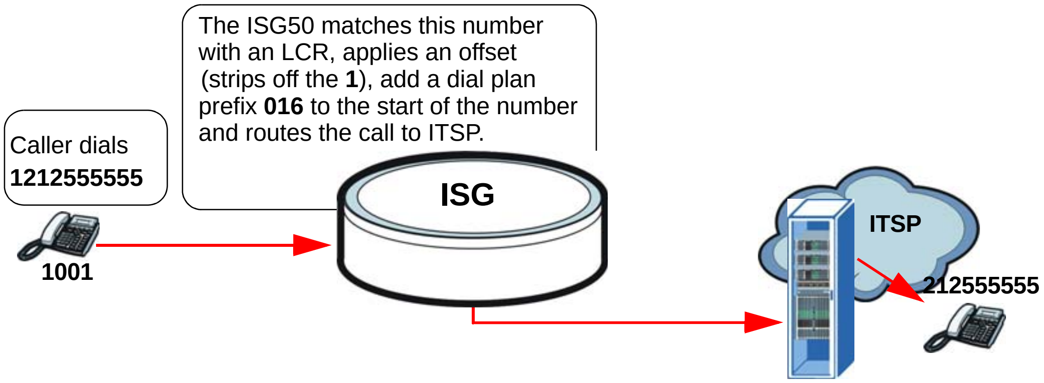

Caller dials 05555555
1001
The ISG50 matches this number with the **LocalCall** LCR, applies the offset (strips off the **0**) and routes the call to PSTN.
ISG
The ISG50 sends the call to **5555555**.
PSTN
5555555

8.4 Making ITSP Calls

The following section shows you how to make and receive calls via a connection to the ITSP. This example covers:

- The ITSP Connection - configuring the outbound line group (connection settings) from the ISG50 to the ITSP.
- Creating a Dialing Rule for ITSP - creating a rule which the tells the ISG50 when to use the ITSP connection when completing outbound calls.

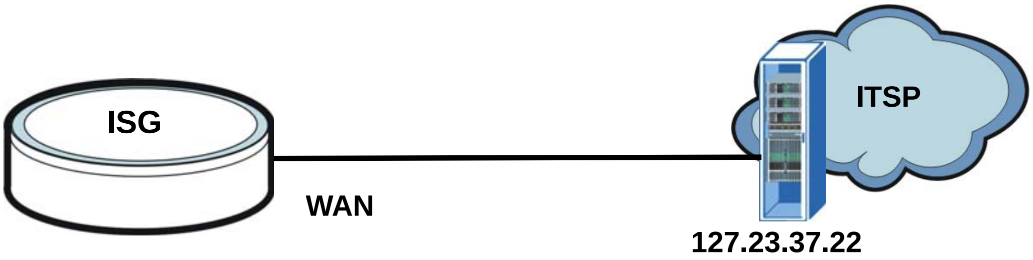
- Assigning an LCR to an Authority Group - giving extensions the right to make outbound calls via the ITSP connection.


The ISG50 matches this number with an LCR, applies an offset (strips off the **1**), add a dial plan prefix **016** to the start of the number and routes the call to ITSP.
Caller dials **1212555555**
ISG
ITSP
1001
212555555

8.4.1 The ITSP Connection

The following section introduces how to configure a connection to the ITSP. This example assumes that the ISG50 has a network connection to the SIP server at your ITSP. The following figure shows the network configuration used in this example.

Figure 120 Network Connection to ITSP

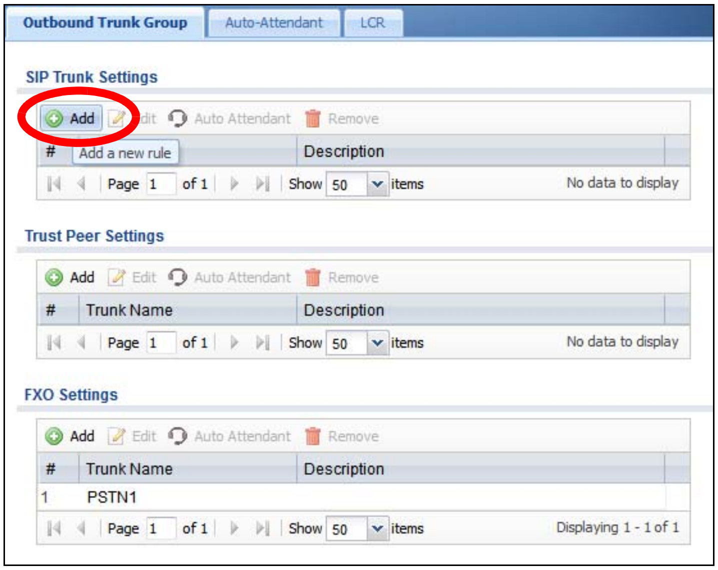

ISG
ITSP
WAN
127.23.37.22

The following table describes sample account information as provided by the ITSP:

Table 20 Sample VoIP Account Information

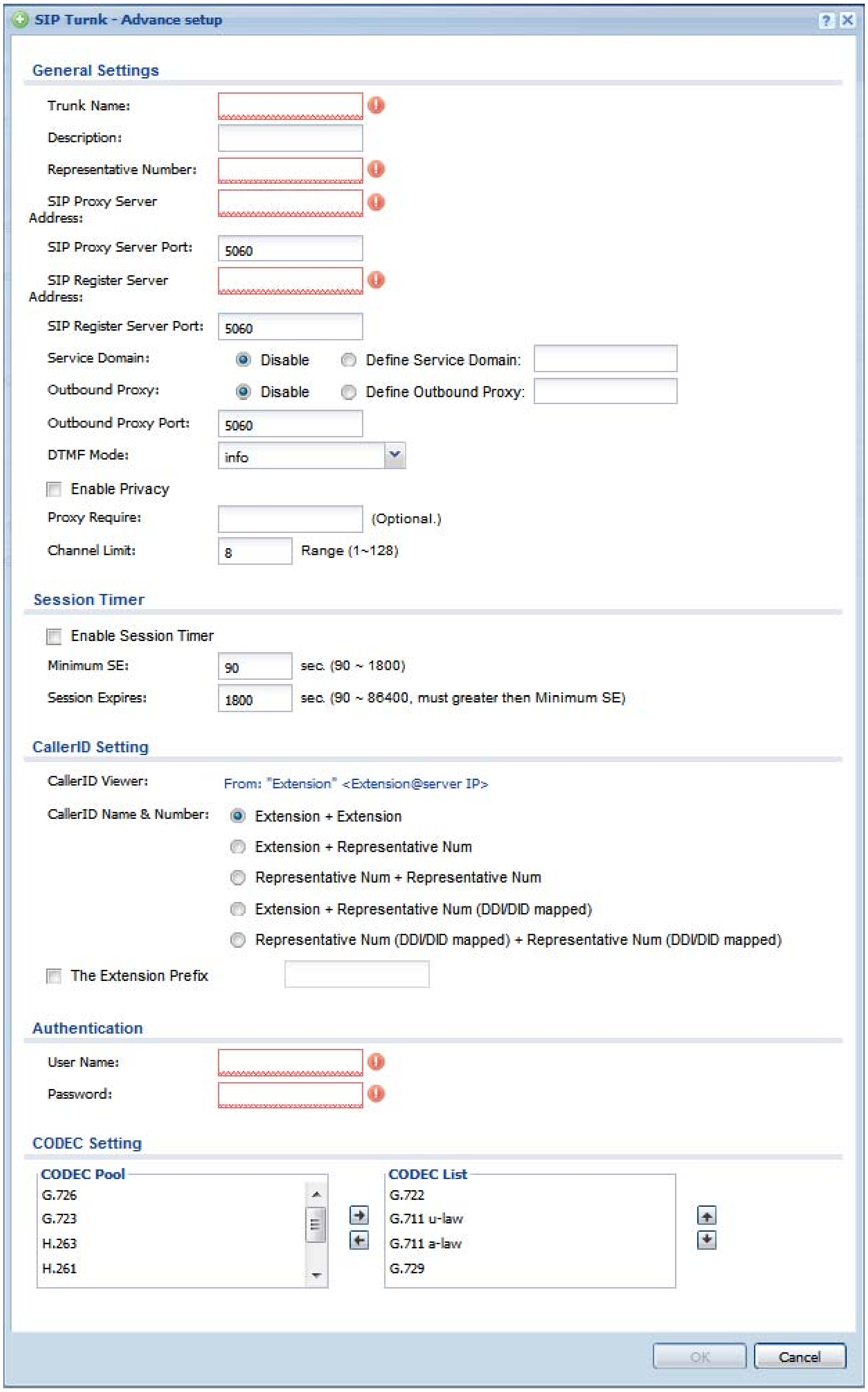
INFO	VALUES		INFO	VALUES
SIP Number (Representative Number)	5551122		SIP Service Domain	127.23.37.22
SIP Server Address	127.23.37.22		DTMF Mode	info
SIP Server Port	5060		SIP Username	5551122
Register Server Address	127.23.37.22		SIP Password	1234
Register Server Port	5060		Codecs supported	G.722, G.726, G.711 u-law, G.711 a-law, G.729A

1 In the web configurator, click **Configuration** > **PBX** > **Outbound Line Management** > **Outbound Line Group**.


Outbound Trunk Group
Auto-Attendant
LCR
SIP Trunk Settings
Add
Edit
Auto Attendant
Remove
Add a new rule
Page 1 of 1
Show 50 items
No data to display
Trust Peer Settings
FXO Settings
Displaying 1 - 1 of 1

#	Trunk Name	Description
1	PSTN1	

2 Click the **Add** icon in the **SIP Trunk** section. Enter the name of the group ("**ITSP1**" in this example). Fill in the other fields with the information provided by your ITSP (in our example we use the sample information as shown in Table 20 on page 148). Click **OK** when you are done.



SIP Turnk - Advance setup

General Settings

Trunk Name:
Description:
Representative Number:
SIP Proxy Server Address:
SIP Proxy Server Port: 5060
SIP Register Server Address:
SIP Register Server Port: 5060
Service Domain: ● Disable ○ Define Service Domain:
Outbound Proxy: ● Disable ○ Define Outbound Proxy:
Outbound Proxy Port: 5060
DTMF Mode: info
☐ Enable Privacy
Proxy Require: (Optional.)
Channel Limit: 8 Range (1~128)

Session Timer

☐ Enable Session Timer
Minimum SE: 90 sec. (90 ~ 1800)
Session Expires: 1800 sec. (90 ~ 86400, must greater then Minimum SE)

CallerID Setting

CallerID Viewer: From: "Extension" <Extension@server IP>
CallerID Name & Number:
● Extension + Extension
○ Extension + Representative Num
○ Representative Num + Representative Num
○ Extension + Representative Num (DDI/DID mapped)
○ Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)
☐ The Extension Prefix

Authentication

User Name:
Password:

CODEC Setting

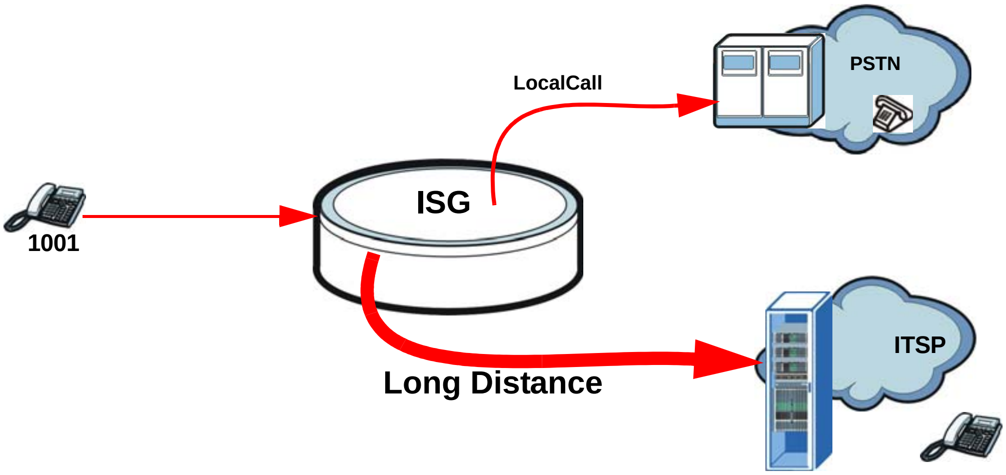
CODEC Pool: G.726, G.723, H.263, H.261
CODEC List: G.722, G.711 u-law, G.711 a-law, G.729

3 People from the outside world can now call the ISG50 using the numbers provided by your ITSP. The default AA prompts the callers to dial the extension they would like to reach. See Section 8.4.2 on page 151 for information on how to set up a dialing rule so that the extensions on your network can make calls via your ITSP.

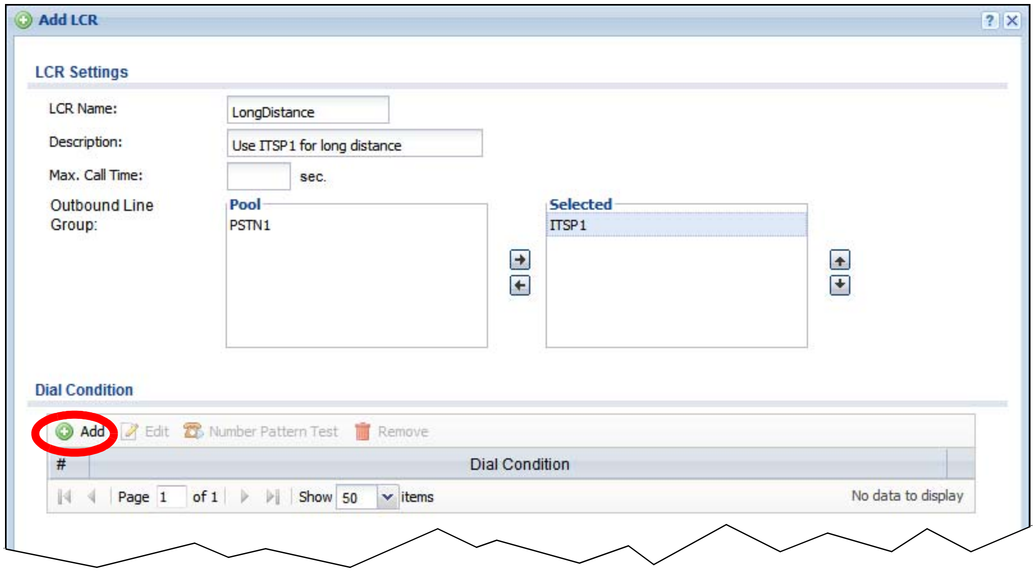
8.4.2 Creating a Dialing Rule for ITSP

In our example we want to use the **ITSP1** outbound line group to complete long distance calls. This is done by configuring the **long_distance_call** LCR. This figure also shows the **LocalCall** LCR we created in Section 8.3.2 on page 144.

Figure 121 Outbound Calls via ITSP


LocalCall
PSTN
ISG
1001
ITSP
Long Distance

1 In the web configurator, click **Configuration > PBX > Outbound Line Management > LCR > Add**. Enter a name and description for the dialing rule (the LCR is named **LongDistance** in this example). Select the outbound line group from the pool column that you want to add to this LCR (in our example this is **ITSP1** as configured in Section 8.4.1 on page 148), then click the **Right** icon to move it to the **Selected** column. Click the **Add** icon to configure a dial condition.


Add LCR
LCR Settings

LCR Name: LongDistance

Description: Use ITSP1 for long distance

Max. Call Time: sec.

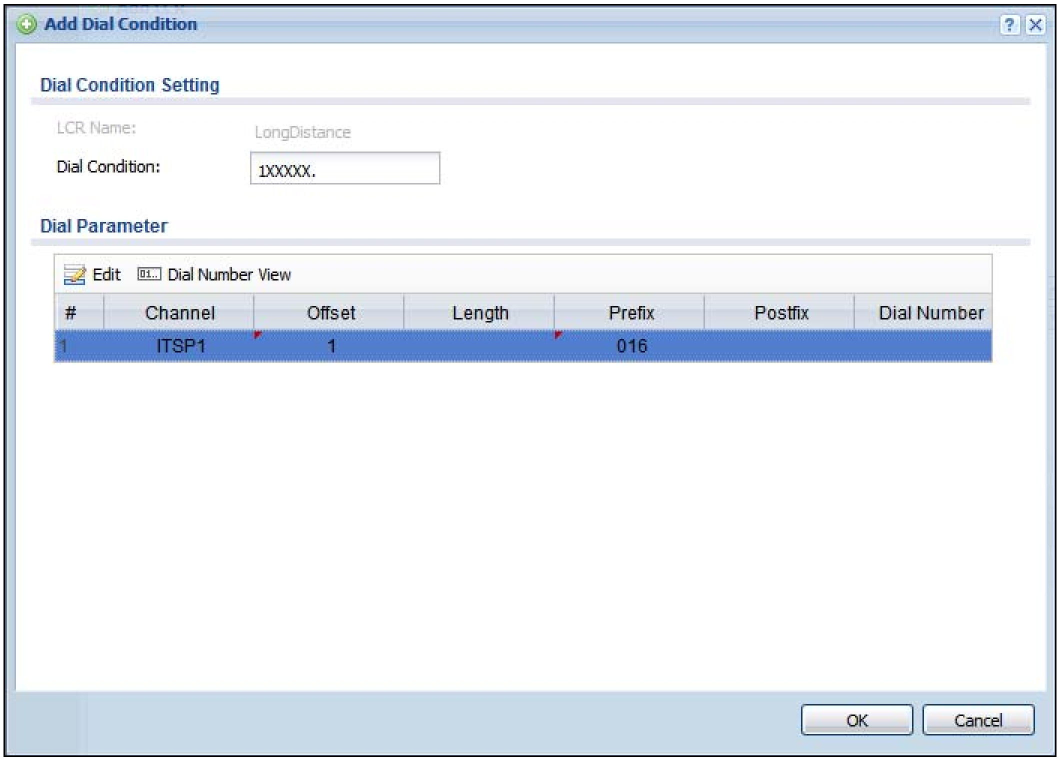
Outbound Line Group:

Pool	Selected
PSTN1	ITSP1

Dial Condition
Add
Edit
Number Pattern Test
Remove
#
Dial Condition
Page 1 of 1
Show 50 items
No data to display

2 The **Dial Condition** screen appears.

- Type **1XXXXX** followed by a period (**.**) in the **Dial Condition** field. This means that this LCR will be used when callers dial any 7 or greater digit number that begins with a **1**. The **X** stands for any digit 0 to 9 and is used to create a minimum length condition. The period (**.**) is a wildcard indicating that any number can follow the **1XXXXX** condition.
- Specify an offset value. In our example, we configure an offset value of **1**. The offset value tells the ISG50 how many initial digits (if any) it should strip off of the dialed number before routing the call to the external line.
- Specify a prefix number. In this example, our ITSP has a special dial plan for long distance calls. A caller must dial **016** in order to take advantage of the dial plan. By adding **016** in the **Prefix** field, the ISG50 automatically adds **016** to calls that match this dial condition. See Figure 3 on page 154 for an example.
- Test the dial condition. Select the dial condition parameter entry and click **Number Pattern Test** to check whether a number dialed from one of the extensions meets the criteria specified in the **Dial Condition** field. In the pop-up window, type a number in the **Number Pattern Test** field and click the right arrow button. An O appears, if the number you typed matches the dial condition. An X appears, if the number you typed does not match the dial condition. In our example, we tested the number **1212555555** to see if it matches our dial condition.
- Click **Apply** to save your settings.



Dial Condition Setting

LCR Name: LongDistance

Dial Condition: 1XXXXX.

Dial Parameter

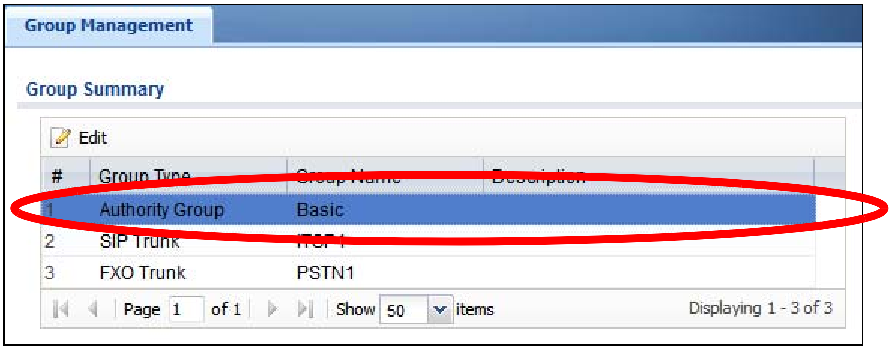
#	Channel	Offset	Length	Prefix	Postfix	Dial Number
1	ITSP1	1		016		

3 You are done configuring the LCR. However, before it can be used by any of the phones connected to the ISG50, the LCR needs to be assigned to an appropriate authority group.

8.4.3 Assigning an LCR to an Authority Group

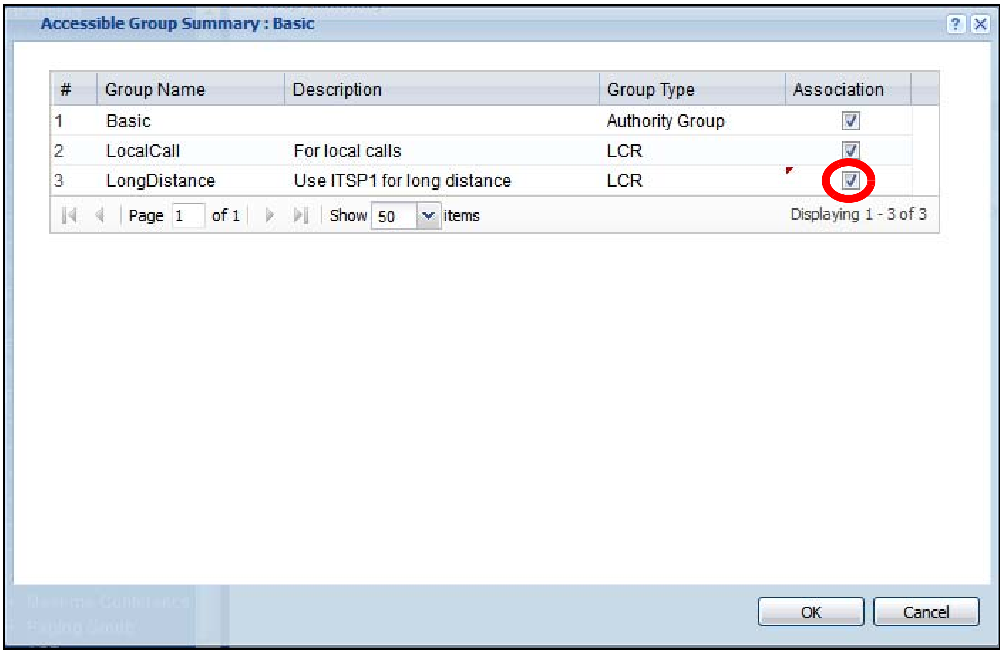
The **Group Management** screen allows you to give an authority group (and the extensions in that group) the right to use an LCR (outbound dial condition). In our example, we give the authority group **Basic** the right to call out using the **LongDistance** LCR.

1 Click **Configuration** > **PBX** > **Group Management** and double-click the **Basic** entry.


Group Management
Group Summary
Edit
Page 1 of 1
Show 50 items
Displaying 1 - 3 of 3

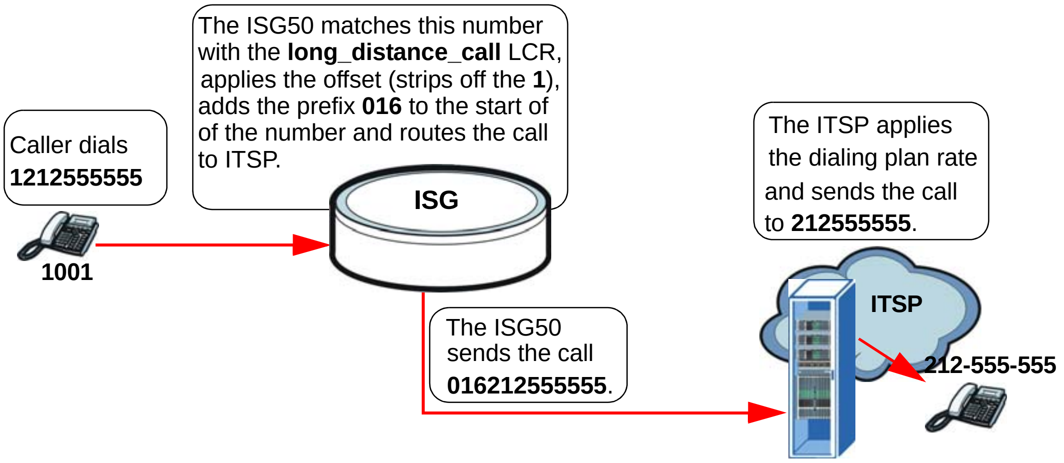
#	Group Type	Group Name	Description
1	Authority Group	Basic	
2	SIP Trunk	ITSP1	
3	FXO Trunk	PSTN1	

2 Select the **LongDistance** entry's checkbox in the **Association** column and click **OK**.


Accessible Group Summary : Basic
Page 1 of 1
Show 50 items
Displaying 1 - 3 of 3
OK
Cancel

#	Group Name	Description	Group Type	Association
1	Basic		Authority Group	☑
2	LocalCall	For local calls	LCR	☑
3	LongDistance	Use ITSP1 for long distance	LCR	☑

3 You can now use the telephones that are part of the **Basic** authority group to make long distance calls using the ITSP connection. The following figure summarizes the outbound call process for this example.


Caller dials **1212555555**

The ISG50 matches this number with the **long_distance_call** LCR, applies the offset (strips off the **1**), adds the prefix **016** to the start of of the number and routes the call to ITSP.

The ISG50 sends the call **016212555555**.

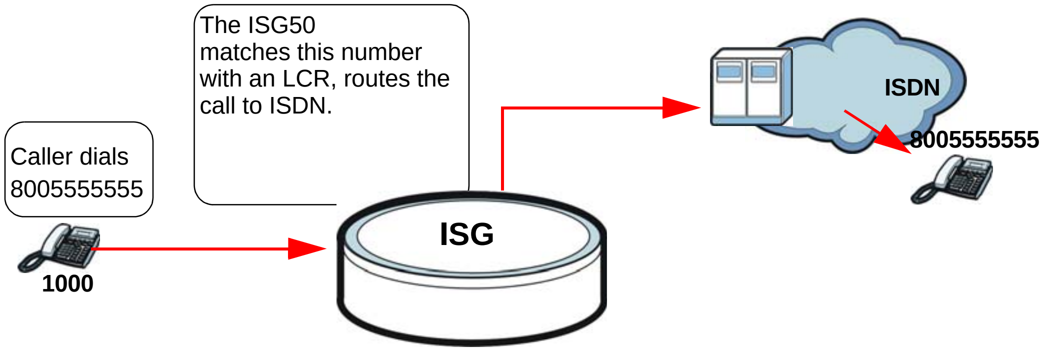
The ITSP applies the dialing plan rate and sends the call to **212555555**.

8.5 Making ISDN Calls

The following section shows you how to make and receive calls via a connection to the ISDN. This example covers:

- The ISDN Connection - configuring the outbound line group’s connection settings from the BRI interface to the ISDN.
- Creating a Dialing Rule for ISDN - creating a rule which tells the ISG50 when to use the ISDN connection when completing outbound calls.
- Assigning an LCR to an Authority Group - giving extensions the right to make outbound calls via the ISDN connection.

Figure 122 Making an ISDN Call

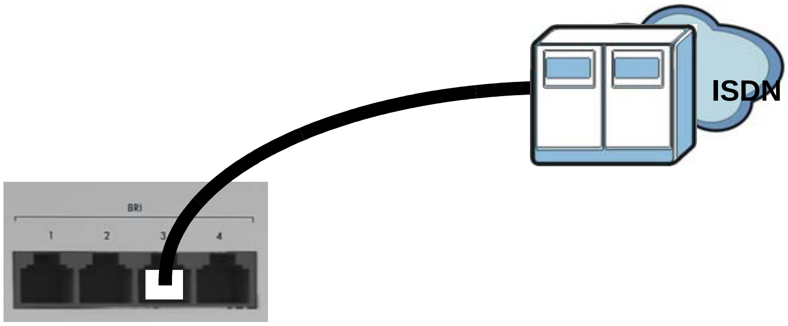

The ISG50 matches this number with an LCR, routes the call to ISDN.

Caller dials 8005555555

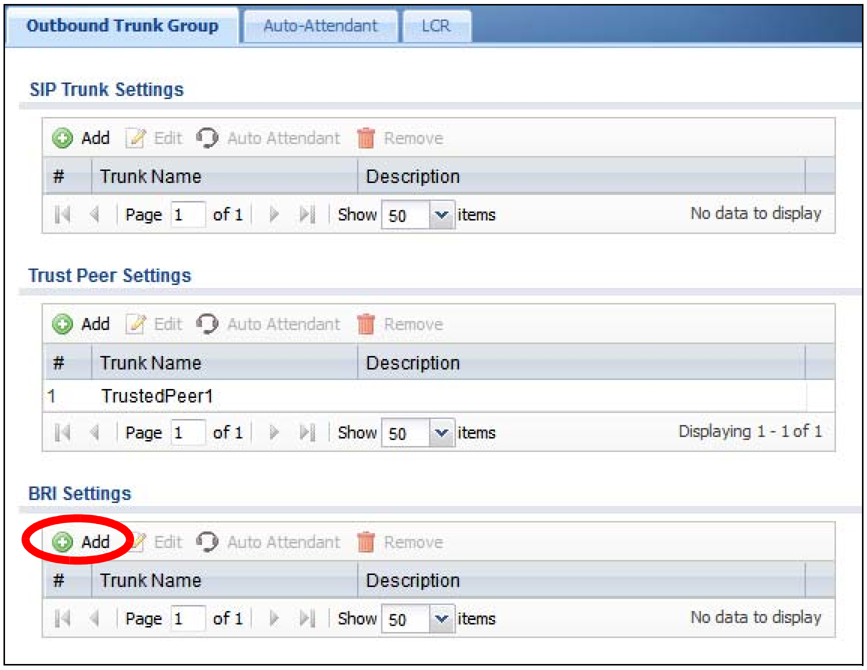
8.5.1 The ISDN Connection

Refer to the Quick Start Guide to connect your telephone cables to the outlets that connect to your local telephone company. The front of your ISG50 should look as shown in the following figure.

Figure 123 BRI Connection


ISDN
BRI
1
2
3
4

1 In the web configurator, click **Configuration > PBX > Outbound Line Management** and click the **Add** icon in the **BRI Settings** section.


Outbound Trunk Group
Auto-Attendant
LCR

SIP Trunk Settings

Add
Edit
Auto Attendant
Remove

#	Trunk Name	Description

Page 1 of 1 | Show 50 items

No data to display

Trust Peer Settings

Add
Edit
Auto Attendant
Remove

#	Trunk Name	Description
1	TrustedPeer1	

Page 1 of 1 | Show 50 items

Displaying 1 - 1 of 1

BRI Settings

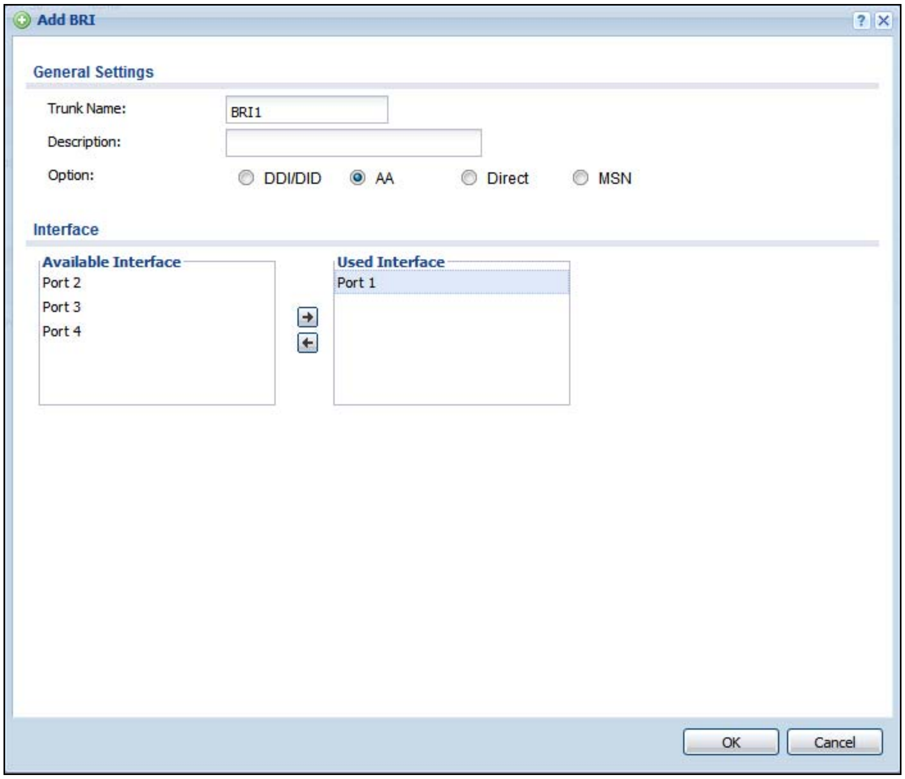
Add
Edit
Auto Attendant
Remove

#	Trunk Name	Description

Page 1 of 1 | Show 50 items

No data to display

2 Enter the name of the group (**BRI1** in this example). Assume you want calls to be answered by the Auto-Attendant, so select **AA**. Select the BRI ports that are to be members and click **OK**.



Add BRI
? X
General Settings

Trunk Name: BRI1

Description:

Option: ○ DDI/DID ● AA ○ Direct ○ MSN

Interface
Available Interface
Port 2
Port 3
Port 4
Used Interface
Port 1
OK
Cancel

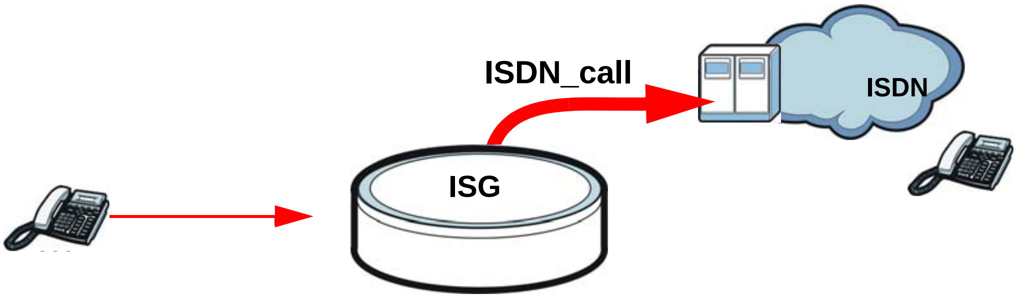
3 People from the outside world can now call the ISG50 using the ISDN numbers provided by your local telephone company. The **Default AA** prompts the callers to dial the extension they would like to reach. See Section 8.5.2 on page 156 for information on how to set up a dialing rule so that the extensions on your network can connect to the ISDN.

8.5.2 Creating a Dialing Rule for ISDN

The following sections show you how to create outbound dialing rules (also referred to as Least Cost Routing or LCR).

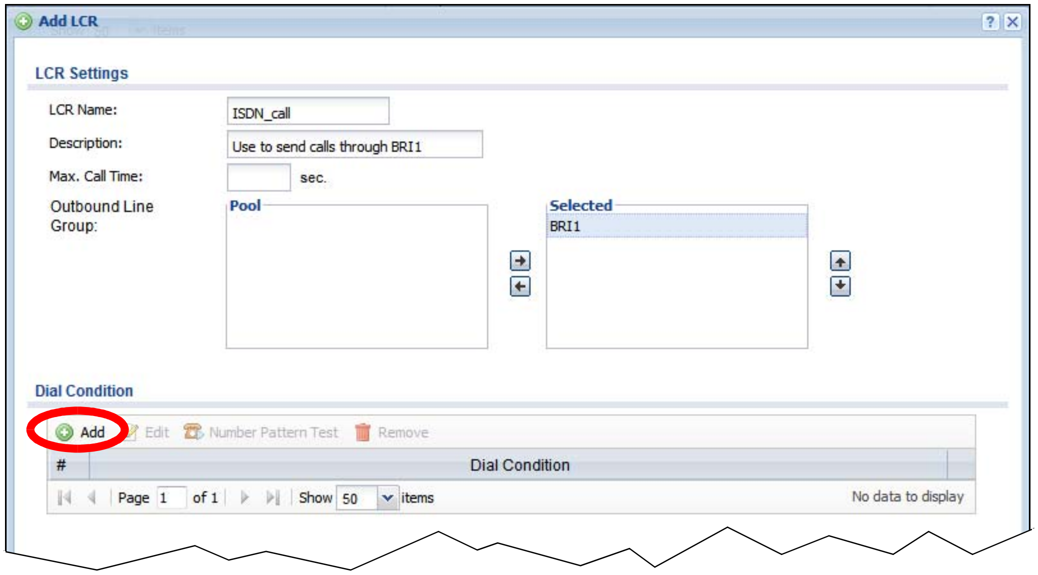
The LCRs determine which outside line the ISG50 should use to complete outbound calls. In our example we want to use the **BRI1** outbound line group to complete local calls.

Figure 124 Outbound Calls via ISDN



ISDN_call
ISDN
ISG

1 In the web configurator, click **Configuration > PBX > Outbound Line Management > LCR > Add**. Enter a name and description for the dialing rule (the LCR is named **ISDN_call** in this example). Select the outbound line group from the pool column that you want to add to this LCR (in our example this is **BRI1** as configured in Section 8.5.1 on page 155), then click the **Right** icon to move them to the **Selected** column. Click the **Add** icon to configure a dial condition.



LCR Name: ISDN_call

Description: Use to send calls through BRI1

Max. Call Time: sec.

Outbound Line Group: Pool / Selected: BRI1

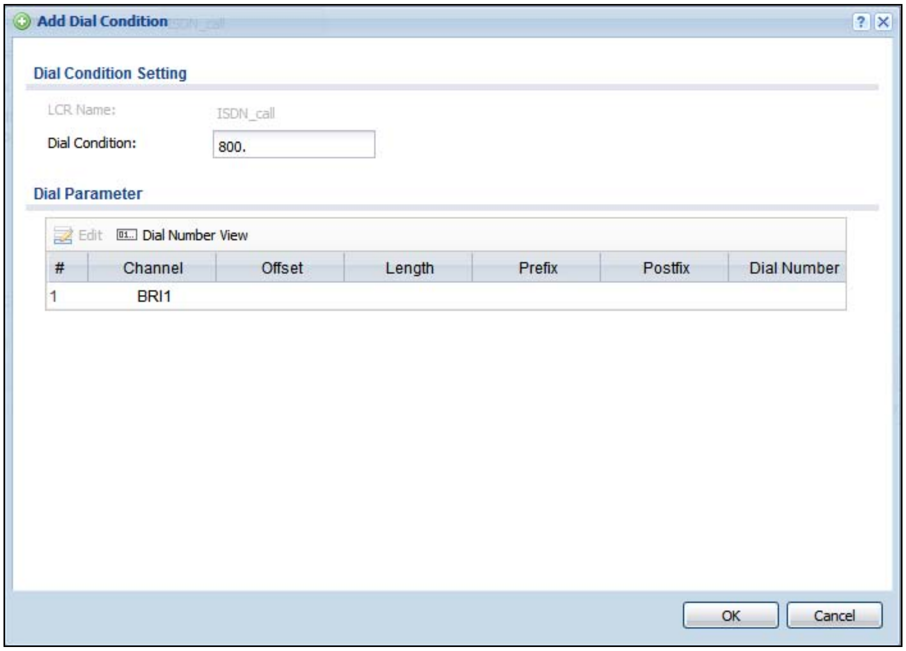
#	Dial Condition

Page 1 of 1 | Show 50 items | No data to display

2 The **Dial Condition** screen appears.

- Type **800** followed by a period (**.**) in the **Dial Condition** field. This means that this LCR will be used when callers dial any number that begins with **800**. The period (**.**) is a wildcard character, meaning anything can follow the 800.
- Leave the offset value empty. In our example, we do not need to configure the offset value. See Figure 124 on page 156 for an example.
- Select the dial condition parameter entry and click **Number Pattern Test** to check whether a number dialed from one of the extensions meets the criteria specified in the **Dial Condition** field. In the pop-up window, type a number in the **Number Pattern Test** field and click the right arrow button. An O appears, if the number you typed matches the dial condition. An X appears, if the number you typed does not match the dial condition. In our example, we tested the number **8005555555** to see if it matches our dial condition.

- Click **OK**.


Add Dial Condition
Dial Condition Setting
Dial Parameter
Edit
Dial Number View
OK
Cancel

LCR Name: ISDN_call

Dial Condition: 800.

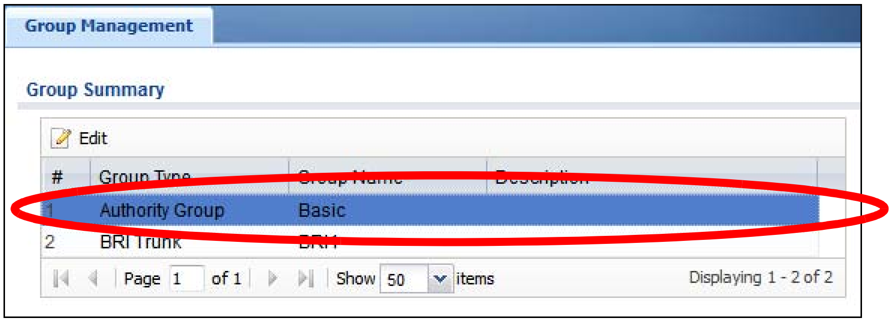
#	Channel	Offset	Length	Prefix	Postfix	Dial Number
1	BRI1					

3 Click **OK** again and you are done configuring the LCR. However, before it can be used by any of the phones connected to the ISG50, the LCR needs to be assigned to an appropriate authority group.

8.5.3 Assigning an LCR to an Authority Group

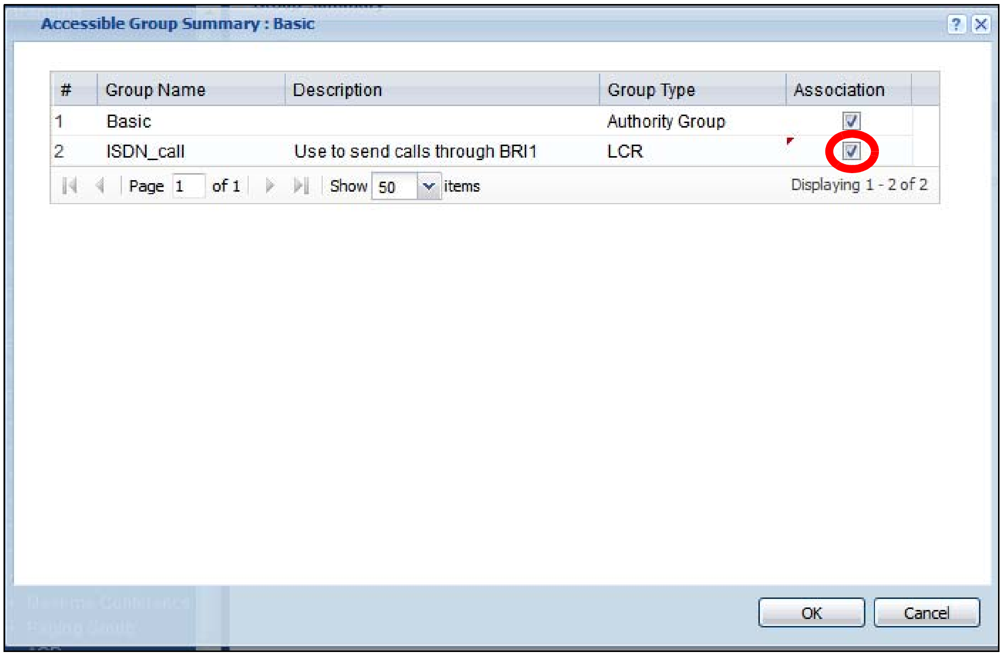
The **Group Management** screen allows you to give an authority group (and the extensions in that group) the right to use an LCR (outbound dial condition). In our example, we give the authority group **Basic** the right to call out using the LCR **ISDN_call**.

1 Click **Configuration** > **PBX** > **Group Management** and double-click the **Basic** entry.


Group Management
Group Summary
Edit
Page 1 of 1
Show 50 items
Displaying 1 - 2 of 2

#	Group Type	Group Name	Description
1	Authority Group	Basic	
2	BRI Trunk	BRI1	

2 Select the **ISDN_call** entry's checkbox in the **Association** column and click **OK**.

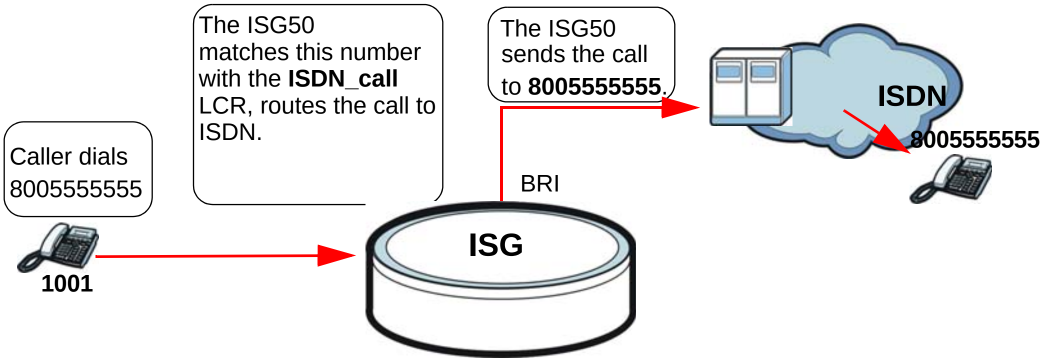


Accessible Group Summary : Basic

#	Group Name	Description	Group Type	Association
1	Basic		Authority Group	☑
2	ISDN_call	Use to send calls through BRI1	LCR	☑

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

3 You can now use the telephones that are part of the **Basic** authority group to make outbound calls using the ISDN connection. The following figure summarizes the outbound call process for this example.

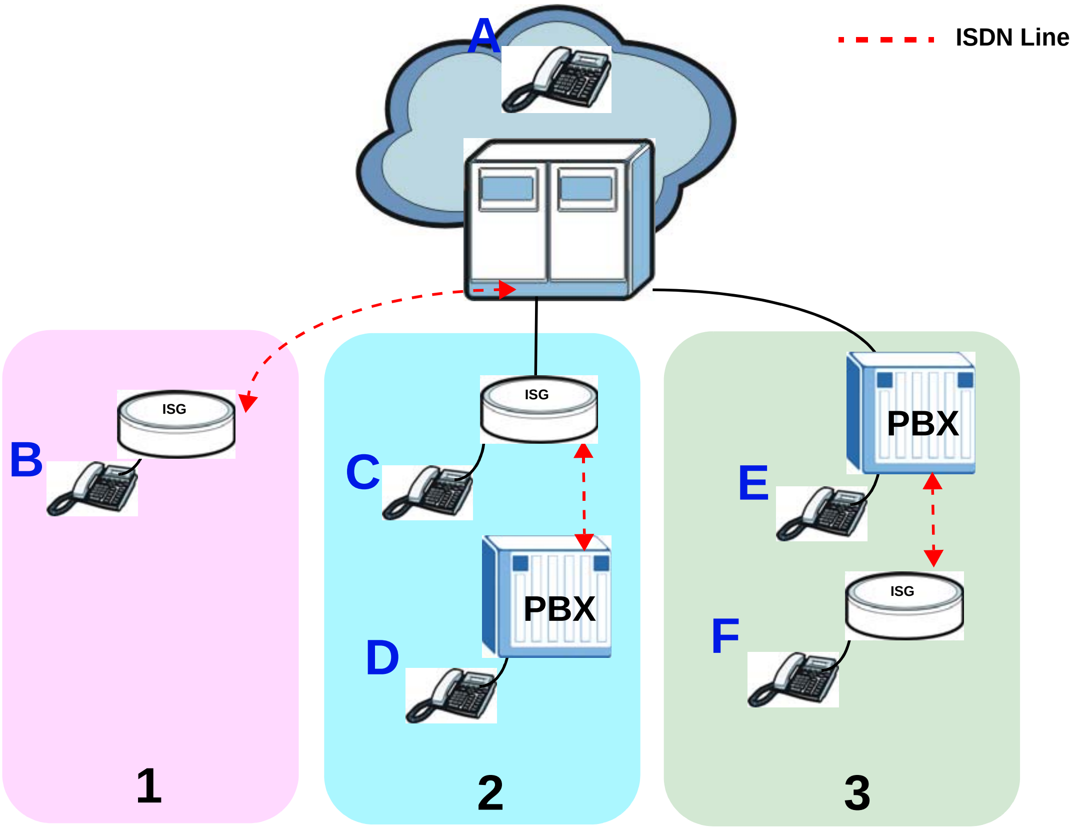

Caller dials 8005555555
1001
The ISG50 matches this number with the **ISDN_call** LCR, routes the call to ISDN.
The ISG50 sends the call to **8005555555**.
BRI
ISG
ISDN
8005555555

8.6 ISDN Network Configuration Examples

The following section shows you some examples of deploying the ISG50 using ISDN in organizations of various sizes.

The following figure shows the three examples (**1** ~ **3**).

Figure 125 ISDN Network Configuration

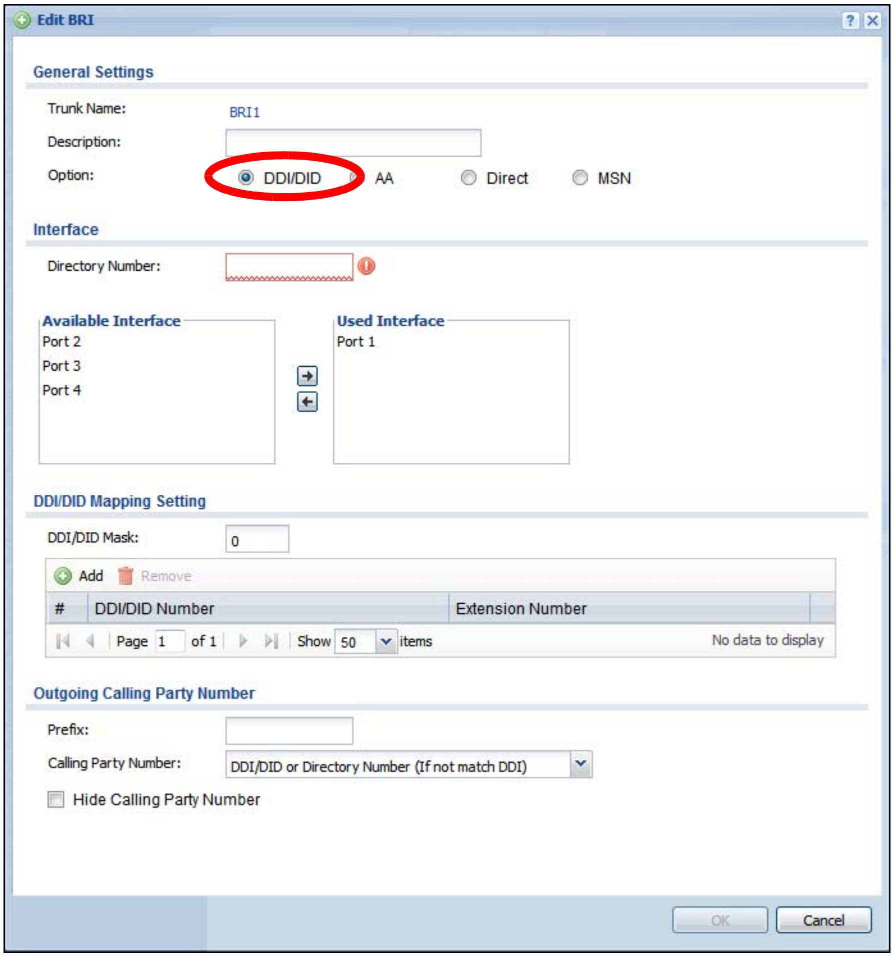


8.6.1 Example 1: Small/Medium Business

For a small/medium company, the ISG50 is the only device that forwards ISDN calls between the company and the telephone service provider.

- For an example of configuring ISDN settings, see Section 8.5 on page 154.

- If you want outsiders to dial in directly to extensions without going through the Auto-Attendant, follow the instructions until step 2, select **DDI/DID** and configure the settings as following.



Edit BRI

General Settings

Trunk Name: BRI1

Description:

Option: ● DDI/DID ○ AA ○ Direct ○ MSN

Interface

Directory Number:

Available Interface: Port 2, Port 3, Port 4

Used Interface: Port 1

DDI/DID Mapping Setting

DDI/DID Mask: 0

#	DDI/DID Number	Extension Number

Page 1 of 1 Show 50 items No data to display

Outgoing Calling Party Number

Prefix:

Calling Party Number: DDI/DID or Directory Number (If not match DDI)

☐ Hide Calling Party Number

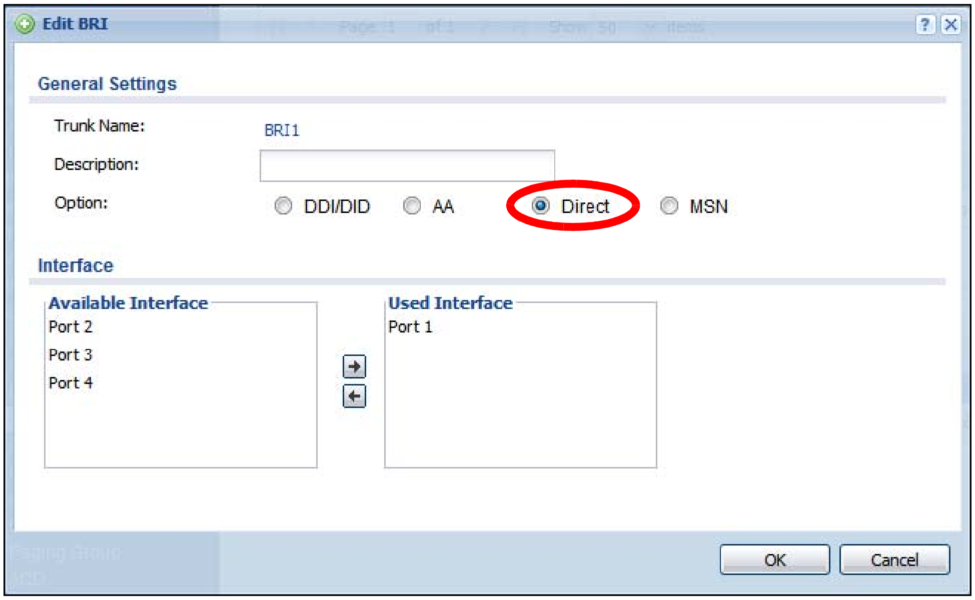
In the **DDI/DID Mapping Setting** section, define **DDI/DID Mask** (the digits of the **Directory Number** on the right) for extension mappings. For example, you define **4** for the DDI/DID Mask and add **1001** to **1001** for the mapping rule. So an incoming call to 8005551001 will be forwarded to the extension.

8.6.2 Example 2: Company with Existing PBX

For a company which already has a PBX. The ISG50 is deployed between the PBX and the telephone service provider. You can connect the ISG50 to the telephone service provider using PSTN connection (see Section 8.3 on page 143) or ISDN (see Section 8.5 on page 154).

If you want the callers from the PBX's extensions not to go through the Auto-Attendant, select one of the following settings and continue the other settings according the instruction.

- If you don't want incoming calls to go through the Auto-Attendant, select **Direct**.



Trunk Name: BRI1

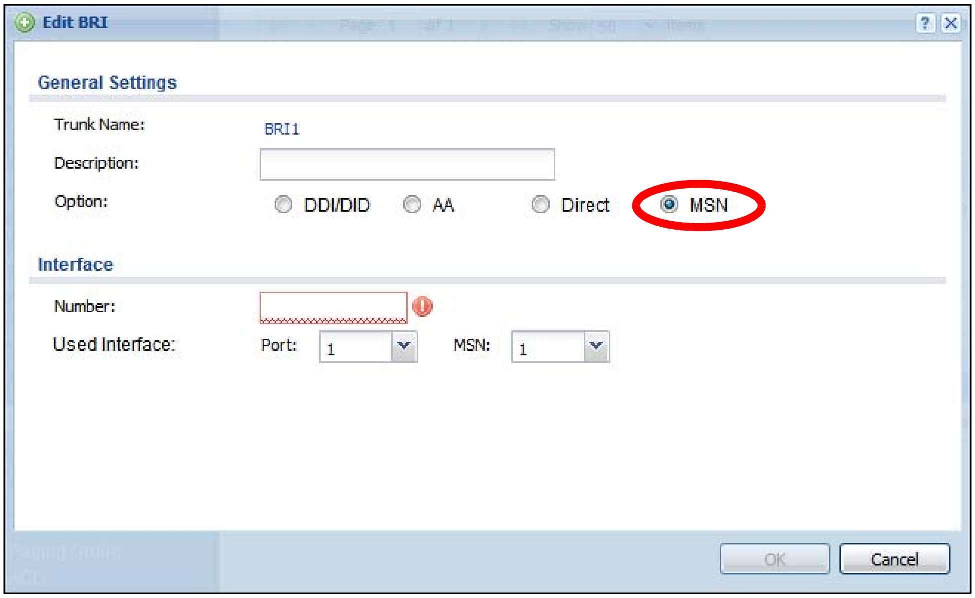
Description:

Option: ○ DDI/DID ○ AA ● Direct ○ MSN

Available Interface: Port 2, Port 3, Port 4

Used Interface: Port 1

- If you are using BRI line(s) and you want to have multiple subscriber numbers on one port, select **MSN** and configure the settings.



Trunk Name: BRI1

Description:

Option: ○ DDI/DID ○ AA ○ Direct ● MSN

Number:

Used Interface: Port: 1 MSN: 1

Note: We don't use DDI/DID in this type of example because DDI/DID is mainly used for outsiders to call extensions.

8.6.3 Example 3: Company with Existing PBX and Expanding Employees

For a company which has a PBX, and is expanding to include more employees, or a new branch office (for example). The ISG50 is behind the PBX system connected using a BRI line.

- See an example of configuring ISDN settings in Section 8.5 on page 154.

- Like Example 2, you can also select **Direct** (if you want the callers from the PBX's extensions to the ISG50's not to go through the Auto-Attendant) or **MSN** (if you are using BRI line(s) and you want to have multiple subscriber numbers on one port).

Note: Like **Example 2**, we don't use DDI/DID in this type of example because DDI/DID is mainly used for outsiders to call extensions.

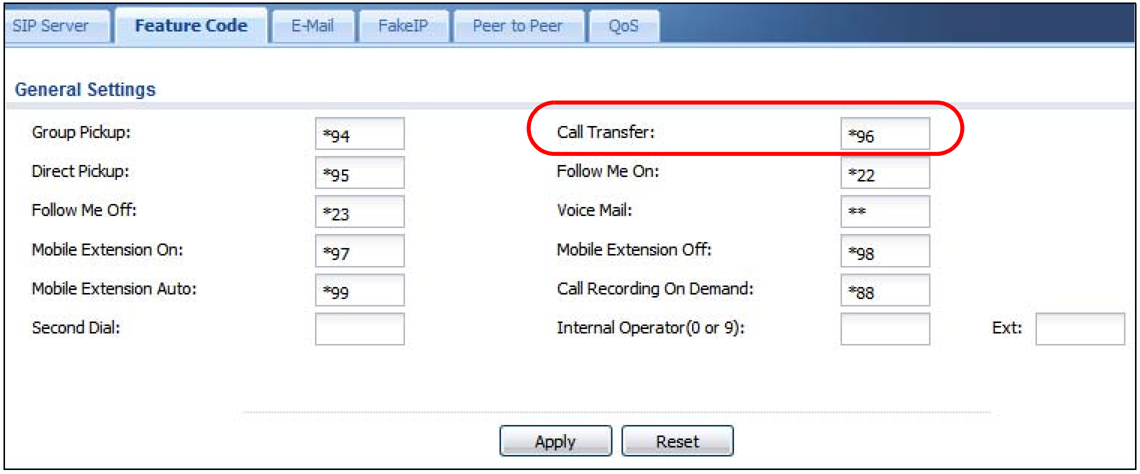
8.7 Using Call Features

The ISG50 has built-in call features for functions such as call forwarding, call blocking, voicemail and so on. These features can be activated or accessed by dialing specific numbers from the phones connected to the ISG50. The numbers used to access call features are called call feature codes. This section shows you how to customize call features. It also describes how to configure a ZyXEL IP phone (V300 is used in our example) to access voicemail by using the voicemail feature code. See Section 27.3 on page 433 for more information on all call features.

8.7.1 Customizing Feature Codes

Click **Configuration > PBX > Global > Feature Code** to display the codes used for the ISG50's call features. You can change the codes in this screen. Provide the users with a list of the features and corresponding codes. Users on your network can then dial a code from their telephone to activate a specific feature. For example, dialing ***96** transfers a call.

Figure 126 Server > Feature Code



Group Pickup:	*94	Call Transfer:	*96		
Direct Pickup:	*95	Follow Me On:	*22		
Follow Me Off:	*23	Voice Mail:	**		
Mobile Extension On:	*97	Mobile Extension Off:	*98		
Mobile Extension Auto:	*99	Call Recording On Demand:	*88		
Second Dial:		Internal Operator(0 or 9):		Ext:	

8.7.2 Using the Voicemail Feature

The voicemail feature code as assigned in Section 8.7.1 on page 163 is ** . Users can dial ** followed by their extension number to access their voicemail. For example, a caller from extension **1001** can dial ****1001** to access voicemail messages.

Some IP phones allow you to configure automatic dialing of feature codes to perform common tasks. See your phone's documentation for details.

8.8 Using the Extension Portal

Every phone user has a personal extension portal on the ISG50. You can log in and make changes to your account setup, and IP phone users also use the web phone. The web phone is just like the telephone you usually use to make calls from this extension; you can call all the same numbers in the same way.

The following sections show examples of how to access the ISG50's extension portal, configure your own personal settings, and use the web phone.

8.8.1 Your Information

In this example, your network administrator has given you some information, as shown in the following table. You can also use this table to note down your own personal information, if you like.

Table 21 Your Information

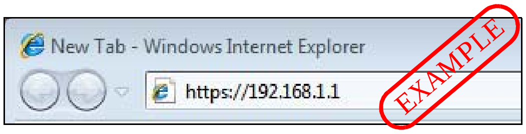
	EXAMPLE INFORMATION	YOUR INFORMATION
Extension Number	1001	
PIN Code	5678	

8.8.2 Accessing the Extension Portal

Take the following steps to access your phone account's extension portal.

Open Internet Explorer and enter "https://" followed by the ISG50's IP address.

Figure 127 Tutorial: Extension Portal IP Address

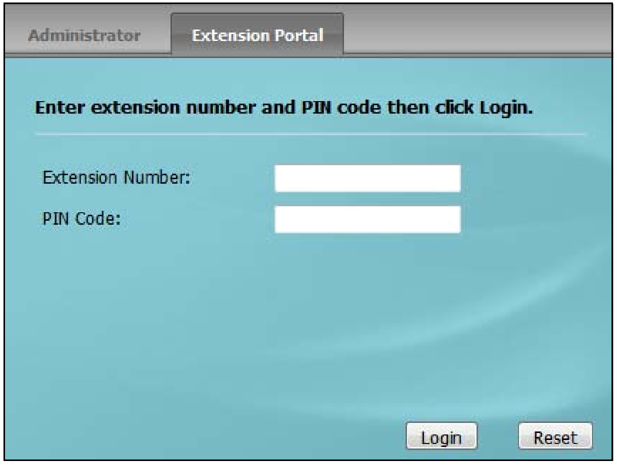


https://192.168.1.1

Note: Don't forget the "s" in "https://" - this "s" indicates a secure IP address, which means that communication between your computer and the ISG50 (including your phone calls) cannot be intercepted by anyone else.

Continue past any warning messages to the **Login** screen. Click the **Extension Portal** tab.

Figure 128 Extension Portal Log In



Enter extension number and PIN code then click Login.

Extension Number:

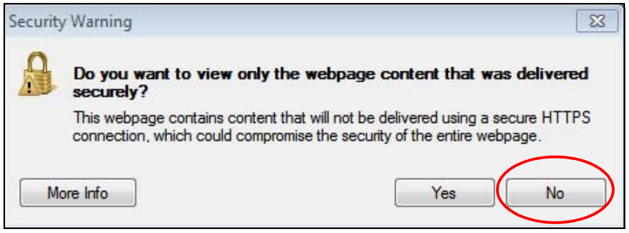
PIN Code:

Enter your extension number (“1001”) in the **Extension Number** field, and enter your PIN code (“5678”) in the **PIN Code** field. Click **SIP Login**.

8.8.3 Using the Web Phone (IP Phone Users Only)

The **Web Phone** screen opens. If a security pop-up screen displays, click the option that lets you view the unsecure content. Some versions of Internet Explorer make this tricky. For example, if the pop-up says “Do you want to view only the webpage content that was delivered securely?”, click **No**.

Figure 129 Tutorial: Security Pop-Up



Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

The **Web Phone** screen displays.

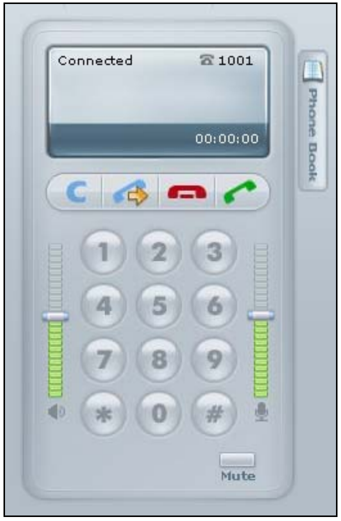


Figure 130 Tutorial: The Web Phone

Note: Make sure you have a headset (or speakers and a microphone) connected to your computer, and that your sound card is working correctly (try listening to an audio file or recording a voice note to check, if there is a problem).

The following table describes how to use the web phone to perform some basic phone functions.

Table 22 Tutorial: Basic Web Phone Call Features

FEATURE	PROCEDURE
Dial a number	Click each numeral using the mouse pointer. The number displays on the screen. Use the “Clear” (C) button to delete a numeral.
Make a call	Dial the number, then click the green “Dial/Pick up” (📞) button on the right.
Receive a call	When a call is incoming, click the green “Dial/Pick up” (📞) button on the right.
End a call	Click the red “Hang up” (☎) button.
Adjust the speaker volume	Use the 🔈 slider on the left of the keypad.
Adjust the microphone volume	Use the 🎤 slider on the right of the keypad.
Mute the speakers and the microphone	Click the **Mute** button below the keypad.
Use the phone book	Click the **Phone Book** tab to the right of the web phone to open the phone book with your contacts list. Click a heading to change the contact list sort order.

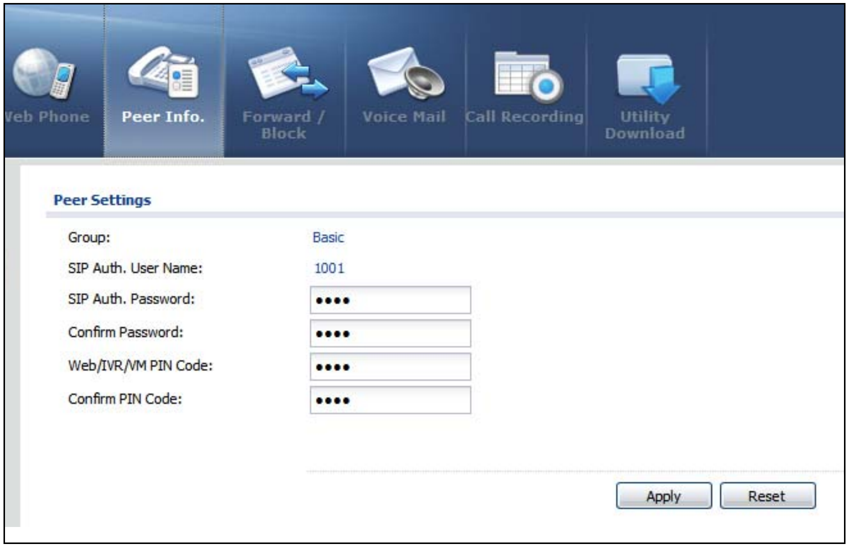
8.8.4 Changing Your Security Information

It is very important that you change your security information as soon as possible, since it could be guessed by others if it was generated automatically.

Click the **Peer Info** tab to change the password for your VoIP account (displayed as **SIP Auth Password**) and the PIN code you use to access the extension portal and voicemail system (displayed as **Web/VM PIN Code**).

Note: The **SIP Auth Password** field does not display if you connect to the ISG50 using a regular analog telephone system.

Figure 131 Tutorial: Changing Security Information



Veb Phone
Peer Info.
Forward / Block
Voice Mail
Call Recording
Utility Download
Peer Settings
Apply
Reset

Group: Basic
SIP Auth. User Name: 1001
SIP Auth. Password: ••••
Confirm Password: ••••
Web/IVR/VM PIN Code: ••••
Confirm PIN Code: ••••

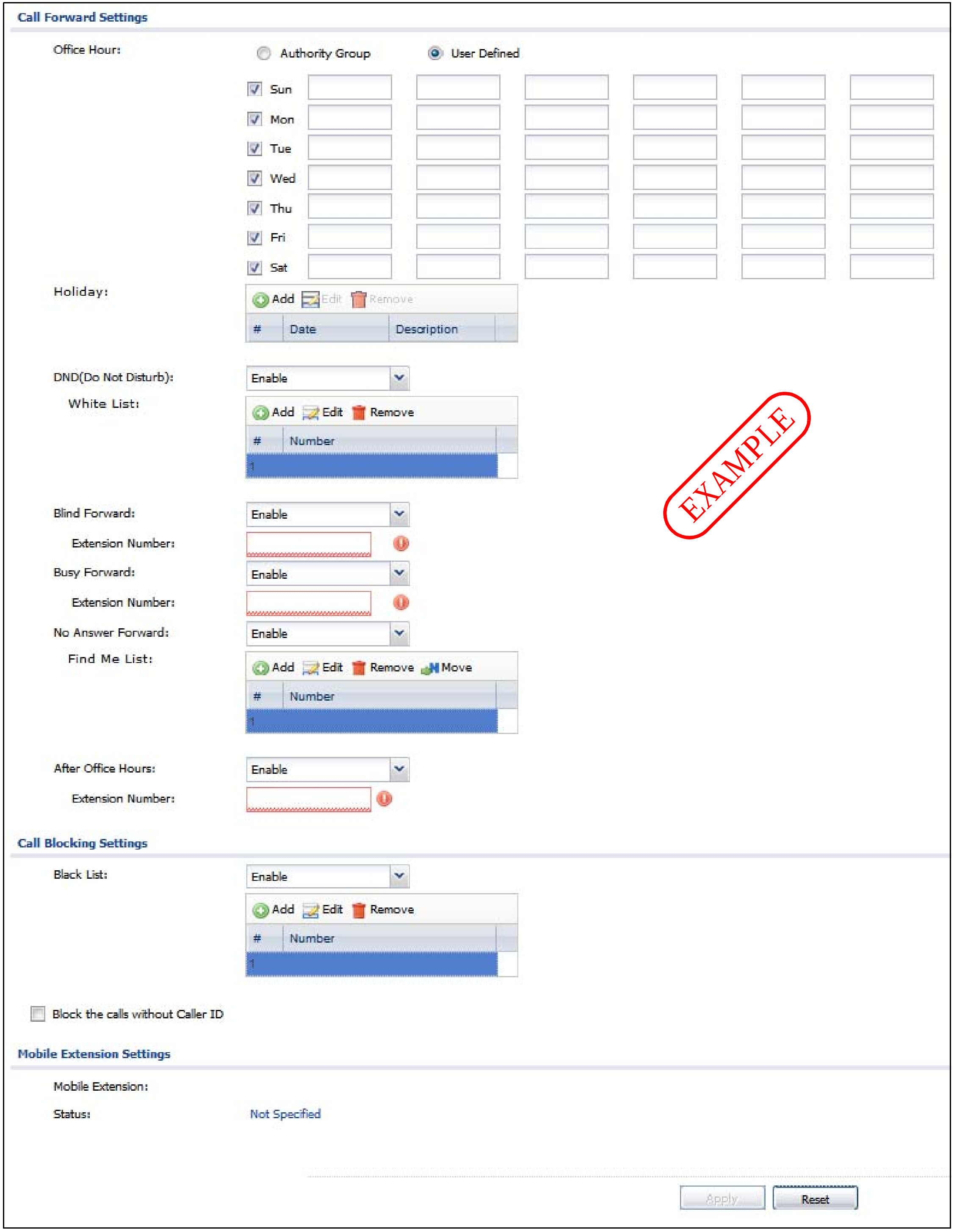
- Enter the new **SIP Auth Password** and enter it again in the next field. Click **Apply**.
- Enter the new **Web/VM PIN Code** and enter it again in the next field. Click **Apply**.

8.8.5 Personalizing Your Settings

Next, configure your extension’s call settings. Click the **Forward/Block** tab at the top of the screen.

The following screen displays.

Figure 132 Tutorial: Configuring Call Settings



Call Forward Settings

Office Hour: ○ Authority Group ● User Defined

☑ Sun
☑ Mon
☑ Tue
☑ Wed
☑ Thu
☑ Fri
☑ Sat

Holiday:

#	Date	Description

DND(Do Not Disturb): Enable

White List:

#	Number
1	

Blind Forward: Enable

Extension Number:

Busy Forward: Enable

Extension Number:

No Answer Forward: Enable

Find Me List:

#	Number
1	

After Office Hours: Enable

Extension Number:

Call Blocking Settings

Black List: Enable

#	Number
1	

☐ Block the calls without Caller ID

Mobile Extension Settings

Mobile Extension:

Status: Not Specified

The following table shows the example call setting information. You can also use this table to make a note of the call settings you want to configure, if you like.

Table 23 Tutorial: Call Settings

	EXAMPLE INFORMATION	YOUR INFORMATION
Office Hours	Monday ~ Friday, 09:00-17:30	
Do Not Disturb (no-one can call you, except for people on the White List)	Disable	
White List (people who can still call you when Do Not Disturb is on)	555 123456 555 234567 555 345678 555 456789	
Call Forwarding (whether or not incoming calls are redirected, and where they are sent)	**Blind Forward**: Disable **Busy Forward**: Voicemail **No Answer Forward**: Find Me List **After Office Hours**: Voicemail	
Find Me List (other extensions where you might be found)	987 654 321	
Black List (people you don't want to call you at all)	555 999888 555 888777	
Block Calls Without Caller ID	Disable	

Take the following steps to configure this screen.

1 **Office Hours**: Ensure that the **Mon** through **Fri** boxes are checked. Clear the **Sat** and **Sun** boxes.

In the **Time** fields, enter **09**:**00-17**:**30**.

2 **Do Not Disturb**: Ensure that **Disable** is selected. You can turn this on later if you want.

3 **White List**: Click the **White List** button. Use the **Add** button to enter each phone number.

4 **Call Forwarding**: Ensure that **Blind Forward** is set to **Disable**. In the **Busy Forward** row, select **Voice Mail**. In the **No Answer Forward** row, select **Enable**. Use the **Add** button in the fields that display to enter each phone number.

In the **After Office Hours** row, select **Voice Mail**.

5 **Black List**: Select **Enable** and click the **Black List** button. Use the **Add** button in the fields that display to enter each phone number.

6 **Block Calls Without Caller ID**: Ensure that **Disable** is selected.

7 Click **Apply**. Your call settings are successfully configured!

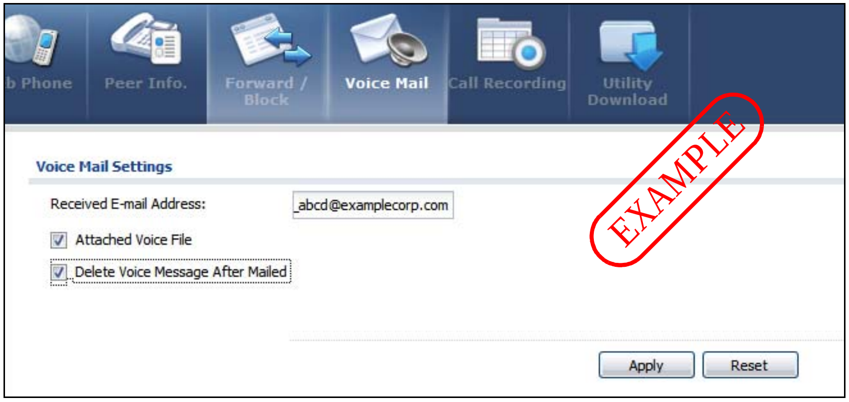
8.8.6 Setting Up Voicemail

Next, you can set up your voicemail inbox to automatically send your received messages as audio files to your email inbox. It is recommended that you do this so that your voicemail inbox does not fill up (if it fills up, no new messages can be recorded).

Click the **Voice Mail** tab at the top of the screen.

The following screen displays.

Figure 133 Tutorial: Setting Up Voicemail



Voice Mail Settings

Received E-mail Address: abcd@examplecorp.com

☑ Attached Voice File

☑ Delete Voice Message After Mailed

The following table shows the example voicemail settings. You can also use this table to make a note of the voicemail settings you want to configure, if you like.

Table 24 Tutorial: Voicemail Settings

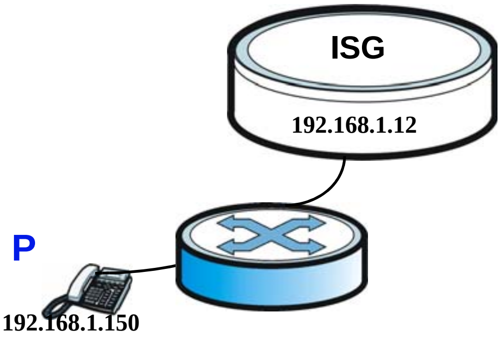
	EXAMPLE INFORMATION	YOUR INFORMATION
Received E-mail Address (the address to which you want the voicemail sent)	user_abcd@examplecorp.com	
Attached Voice File (send the audio file to your email account)	Yes	
Delete Voice Message After Mailed	Yes	

To configure this screen, enter your email address in the **Received E-mail Address** field, select **Attached Voice File** and select **Delete Voice Message After Mailed**. Click **Apply**.

8.9 Capturing Packets Using the Web Configurator

The following section shows you how to capture packets using the ISG50 web configurator. You may need to do this if there are problems. For example, suppose a SIP phone (**P**) fails to register to the ISG50.

Figure 134 Tutorial: Basic Troubleshooting Using Packet Capture

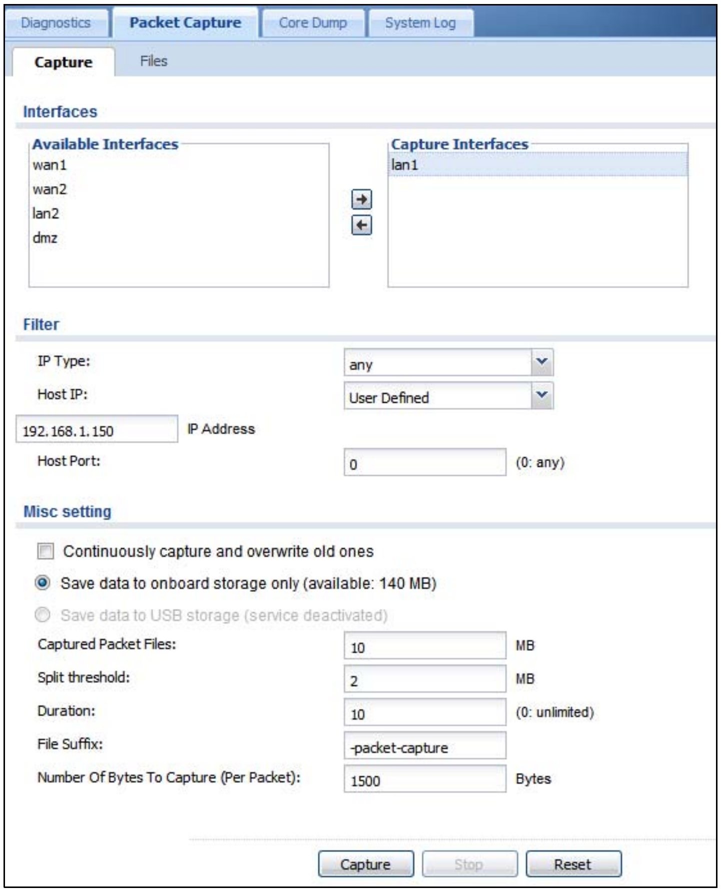


Do the following to capture packets between **P** and the ISG50:

1. Go to **Maintenance** > **Diagnostics** > **Packet Capture** and configure the following:
    - Interface: lan1
    - IP type: All
    - Host IP: 192.168.1.150

- Duration: 10 seconds

Then click **Capture**.


Diagnostics
Packet Capture
Core Dump
System Log
Capture
Files
Capture
Stop
Reset

Interfaces

Available Interfaces: wan1, wan2, lan2, dmz

Capture Interfaces: lan1

Filter

IP Type: any

Host IP: User Defined

192.168.1.150 IP Address

Host Port: 0 (0: any)

Misc setting

☐ Continuously capture and overwrite old ones

● Save data to onboard storage only (available: 140 MB)

○ Save data to USB storage (service deactivated)

Captured Packet Files: 10 MB

Split threshold: 2 MB

Duration: 10 (0: unlimited)

File Suffix: -packet-capture

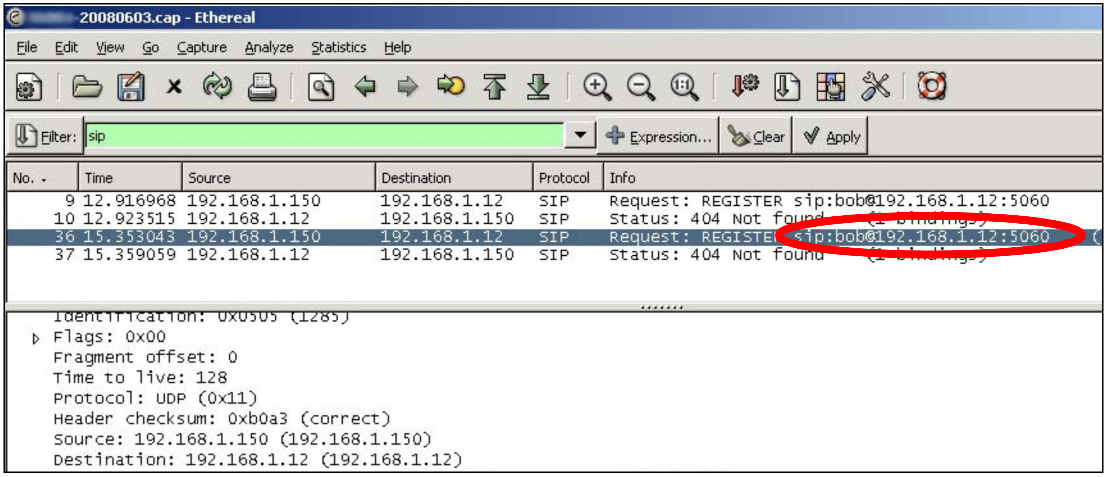
Number Of Bytes To Capture (Per Packet): 1500 Bytes

2 Re-initialize the SIP phone. This helps to get a complete packet capturing.

3 Wait ten seconds, then use the **Files** tab to save the file to your computer.

4 Use a packet capturing tool (such as Ethereal) to open the file and analyze the possible root cause.

In this example, registration fails because the SIP username must be a number and not letters (**bob** in this example) for the ISG50.


[redacted]20080603.cap - Ethereal
File
Edit
View
Go
Capture
Analyze
Statistics
Help
Expression...
Clear
Apply

Filter: sip

```
No. -  Time      Source          Destination     Protocol  Info
     9 12.916968 192.168.1.150   192.168.1.12    SIP       Request: REGISTER sip:bob@192.168.1.12:5060
    10 12.923515 192.168.1.12    192.168.1.150   SIP       Status: 404 Not found    (1 bindings)
    36 15.353043 192.168.1.150   192.168.1.12    SIP       Request: REGISTER sip:bob@192.168.1.12:5060  (
    37 15.359059 192.168.1.12    192.168.1.150   SIP       Status: 404 Not found    (1 bindings)
```

```
    Identification: 0x0505 (1285)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0xb0a3 (correct)
    Source: 192.168.1.150 (192.168.1.150)
    Destination: 192.168.1.12 (192.168.1.12)
```

If you cannot solve the problem, contact customer support and send this file.

You may be asked to provide another file containing more real-time system information. Select **Maintenance** > **Diagnostics** > **Collect** and click **Collect Now**. Wait several seconds, then use the **Files** tab to save the file to your computer.

8.10 Creating an Automated Menu System

The Automatic Call Distribution (ACD) system allows you to set up automated audio menus and the connections between them which will allow incoming phone calls to be routed to the best available people to receive them. For example, if the Acme Widget company sells its products in two different countries (the United States and Mexico), then it would probably want to set up a customer service line that can direct callers based on their language preference.

Before getting started, there are a few ACD-specific terms with which you should familiarize yourself first:

- **Agent** - An agent is a callee, or the person who ultimately receives an incoming call. Agents are grouped according to skills.
- **Skill** - A skill is a specific function that an agent performs. For example, in the Acme Widget company’s customer support department, some of the agents are fluent in English while others are fluent in Spanish. Both English and Spanish are labeled as skills for the purpose of routing calls through the ACD system.
- **Auto-Attendant (AA)** - The auto attendant is the crux of the automated menu system. It functions as a kind of automated switch board operator. When properly configured, the ISG50 auto-attendant can be the foundation of any automatic menu system, replete with custom the audio recordings which the caller hears when first dialing in and keypad-responsive menus which guide them to their intended recipients.

For a full description of all available ACD and Auto-Attendant features on the ISG50, see Chapter 38 on page 553 and Chapter 31 on page 503, respectively.

8.10.1 Menu Design and Call Routing

First, you want to design your call center’s automated audio menu “map”. Start by asking yourself a few key questions, such as: How are calls going to be routed once a person dials the phone number assigned to the system? What is the first level of menus the caller encounters? After the call makes his selection, then what is the second level of menus? After the second level of menus, are calls then sent to an agent?

For the Acme Widget company, the company manger decides he wants to divide the menus up by languages first (English and Spanish), and then skills (Order Status, Technical Support, and Operator) for each language, each of which contains its own set of agents.

In order to do this, he must map his connections:

Table 25 Tutorial: Example Automated Menu Design

1ST MENU	SUBMENUS	SKILLS	AGENTS
Language Selection	English	Order Status	Tom Pam Steven
		Technical Support	Steven George
		Accounts and Billing	George
	Spanish	Estado del Pedido	Eddie Susan Maria
		Apoyo Técnico	Maria Alejandro
		Cuentas y Facturación	Alejandro

- The first menu and the submenus both utilize an auto-attendant. Auto-attendants are set up in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** screen. This portion of the tutorial is described in Section 8.10.4 on page 178.
- The skills are the intermediaries between the AA submenu and the agents. Skills are set up in the **Configuration > PBX > ACD > Skill** screen. This portion of the tutorial is in Section 8.10.3 on page 175.
- The agents associated are the ultimate destination for incoming calls to the system. Agents are set up in the **Configuration > PBX > ACD > Agent** screen. This portion of the tutorial can be found in Section 8.10.2 on page 174.

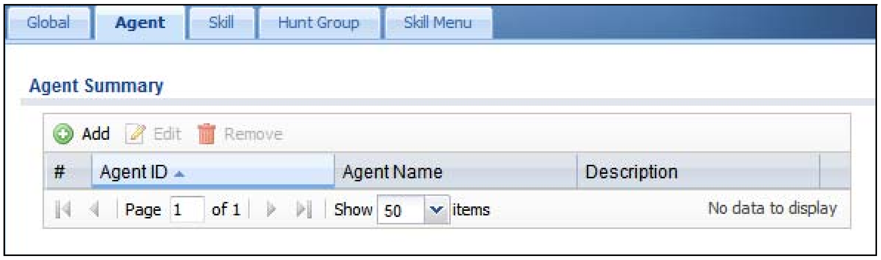
Although the usage order is 1st Menu - Submenus - Skills - Agents, we have to build our system in reverse order by starting with the ACD-based agents and skills and then work our backwards toward the auto-attendant-based menus. This is because the auto-attendant menus require the skills to already be defined when setting them up as part of an automated menu system, while skills require agents to be pre-defined as they are set up.

8.10.2 Create an Agent Identity

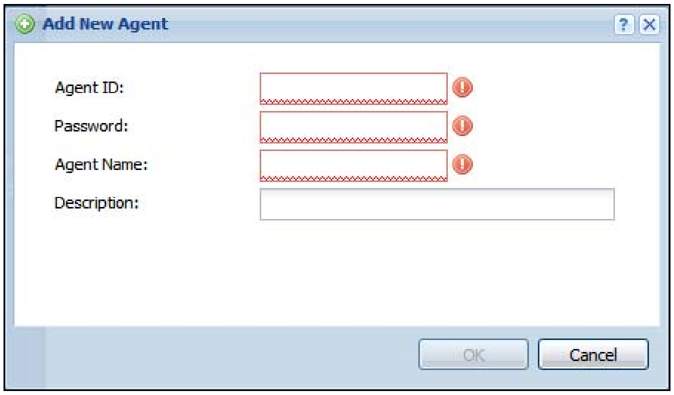
Now that you have more or less mapped out your automated menus and call routes, it’s time to actually start building them on the ISG50. The first thing we’re going to do is create our agent identities. This allows us to assign the agents immediately to skills as we create them in the next section.

To create an agent identity:

1 Log into the ISG50, then go to the **Configuration > PBX > ACD > Agent** screen.


Global
Agent
Skill
Hunt Group
Skill Menu
Agent Summary
Add
Edit
Remove
#
Agent ID
Agent Name
Description
Page 1 of 1
Show 50 items
No data to display

2 For each of your agents, click the **Add** button to open the **Agent Settings** screen, and configure the following items:


Add New Agent
Agent ID:
Password:
Agent Name:
Description:
OK
Cancel

Agent ID: Enter between 3 and 20 digits to serve as the agent's identification number. This number cannot overlap with existing extension numbers and is required for the agent to log into the ACD system from his telephone.

Password: Enter between 1 and 32 digits for the agent's password. As with the Agent ID, this is required to log into the ACD system from an agent's telephone.

Agent Name: Enter between 1 and 32 alphanumeric characters here that will be associated with the skills and skill menus in subsequent sections. While you can use an agent's real name, it is certainly not necessary. In fact, if multiple people log in on the same agent ID, it is recommended you use a more neutral name to identify them (such as 'Accounting' for a team as opposed to 'Julia', who happens to be one accountant on the team).

Description: This field is optional, allowing you to add supplementary information to the agent. This appears on the **Configuration > PBX > ACD > Agent** screen. Enter up to 64 alphanumeric characters.

3 Click **OK** when you are done.

8.10.3 Create a Skill

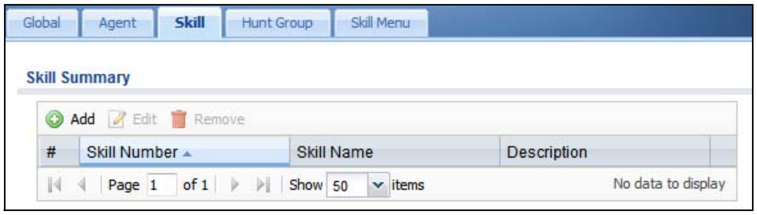
The next step is to define our skills. Doing this second allows us to link the agents we created in the previous section to the skills we're going to create in this section. It also allows us to later assign these very same skills to the auto attendant menus when they are, in turn, created.

In the context of the ISG50, a skill is a set of rules that define how incoming calls are sent to the agents who are associated with that skill. For example, if the Acme Widget company defines

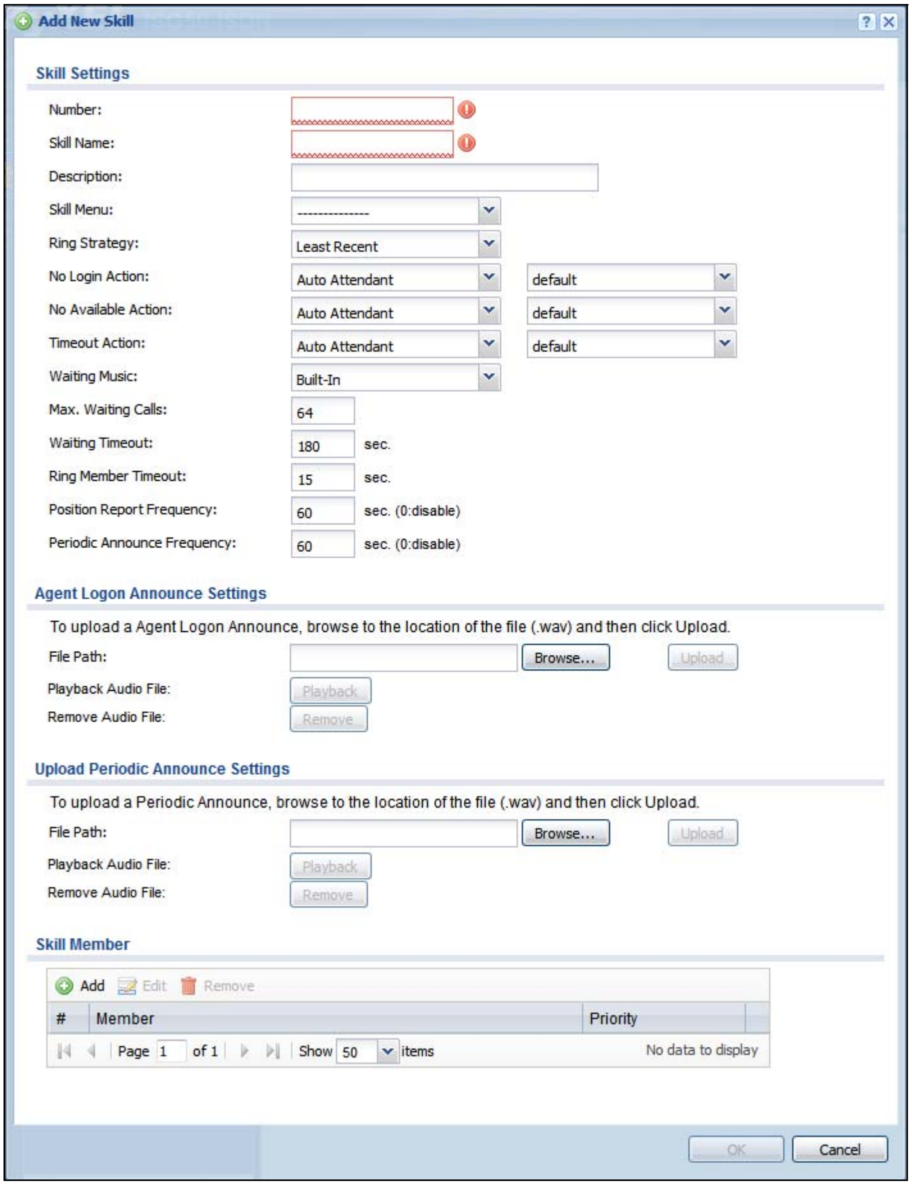
"Technical Support" as a skill, then any caller who presses the key for that skill is immediately forwarded to the first available person whose agent identity appears on that skill's rule list.

To create a new skill:

1 Go to the **Configuration > ACD > Skill** screen.


Global
Agent
Skill
Hunt Group
Skill Menu
Skill Summary
Add
Edit
Remove
#
Skill Number
Skill Name
Description
Page 1 of 1
Show 50 items
No data to display

2 For each skill, click the **Add** button to open the **Add New Skill** screen, and assign configure the following items:



Number:
Skill Name:
Description:
Skill Menu: --------------
Ring Strategy: Least Recent
No Login Action: Auto Attendant, default
No Available Action: Auto Attendant, default
Timeout Action: Auto Attendant, default
Waiting Music: Built-In
Max. Waiting Calls: 64
Waiting Timeout: 180 sec.
Ring Member Timeout: 15 sec.
Position Report Frequency: 60 sec. (0:disable)
Periodic Announce Frequency: 60 sec. (0:disable)

To upload a Agent Logon Announce, browse to the location of the file (.wav) and then click Upload.
File Path:
Playback Audio File:
Remove Audio File:

To upload a Periodic Announce, browse to the location of the file (.wav) and then click Upload.
File Path:
Playback Audio File:
Remove Audio File:

#	Member	Priority

Page 1 of 1 | Show 50 items | No data to display

Number: Enter an identification number of this skill. This is required to link the skill to a skill menu in the next section. You can use between 3 and 20 digits.

Skill Name: Enter a descriptive name for this skill. For example, “Order Status” since this will be the skill that forwards all calls requesting order status information to the appropriate people.

Ring Strategy: This option allows you to choose how a call is forwarded to the agents associated with this skill. When a call comes in, it is not logistically possible for the ISG50 to forward the call to every associated agent. Therefore, a ring strategy must be employed. For example, let’s say we’re configuring the “Order Status” skill. We know from part I that the company manager intends on having two agents linked to this skill (Pam and Steven). He decides that the person who has received the fewest number of incoming calls since logging in should always be the first to answer the next incoming call. He therefore sets the **Ring Strategy** option to **Fewest Calls**. For more information about this option, see Section 38.4.1 on page 559.

No Login Action: This option determines how the ISG50 handles incoming calls to the agents associated with this skill when none of them have logged on yet. The company manager decides to let voice mail pick up missed calls when neither of the agents logs in, and enters the actual telephone extension for Pam.

No Available Action: This is similar to the previous option, but tells the ISG50 how to handle incoming calls to the agents associated with this skill when they are all already engaged in conversation. The company manager knows that not every agent in every skill will be occupied all of the time, and so he chooses **Backup Skill** as the setting for this field. However, until he creates additional skills he will not be able to choose which backup skill takes over in the event all agents associated with this one are busy.

Timeout Action: This is similar to the preceding two options, determining how the ISG50 handles incoming calls when an agent does not answer or pick up after a certain amount of time.

Max Waiting Calls: Enter the maximum number of calls that will be allowed to queue up if the agents are already engaged in conversation. The company manager chooses to let the default of 64 calls remain as it is. In a small office environment, it seems unlikely that they will have an issue with a call backlog.

Skill Member: This is where you select the agents whom you want to link to this skill. The **Priority** determines which people receive calls first (followed by **Ring Strategy**); if two people are set for priority 1 and the third set for priority 2, then the calls are first directed to the priority 1 agents. Only when both of those agents are unavailable do calls get directed to priority 2 agents. In this example, the company manager assigns priority 1 to Tom and Pam and priority 2 to Steven, because Steven also fields call for Technical Support. This way, he won't receive as many calls for Order Status as the other two, giving him more time to field calls for his primary skill.

3 Click **OK** when you are done.

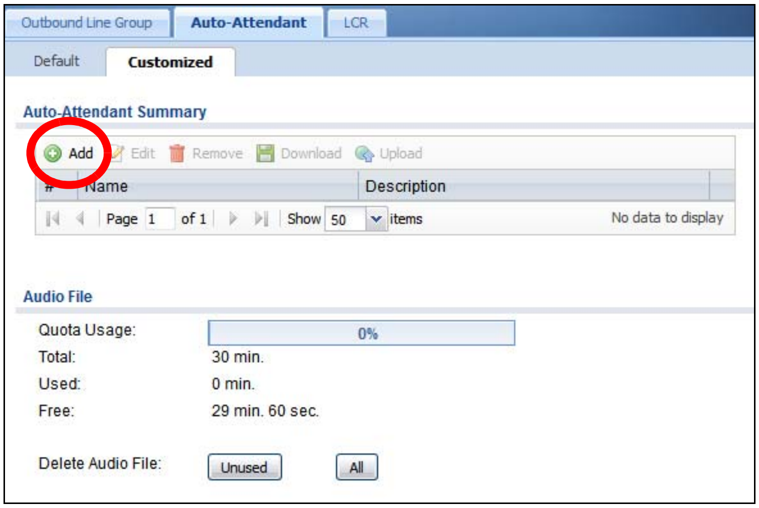
Note: After you create a number of skills, you may want to edit them again to update the **No Logon Action**, **No Available Action** and **Timeout Action** fields if they use the **Backup Skill** setting.

8.10.4 Create an Auto-Attendant

The final step in building our automated menu system is to configure our auto-attendant. For the Acme Widget company, we require two auto-attendants: one to handle the first menu tier (English / Spanish) and another to handle the submenu tier (Skills). Once a caller gets to the submenu, his call can then be forwarded to a live person, or in other words, an agent.

1 Go to the **Configuration > PBX > Outbound Line Management > Auto-Attendant** screen then select the **Customized** tab.

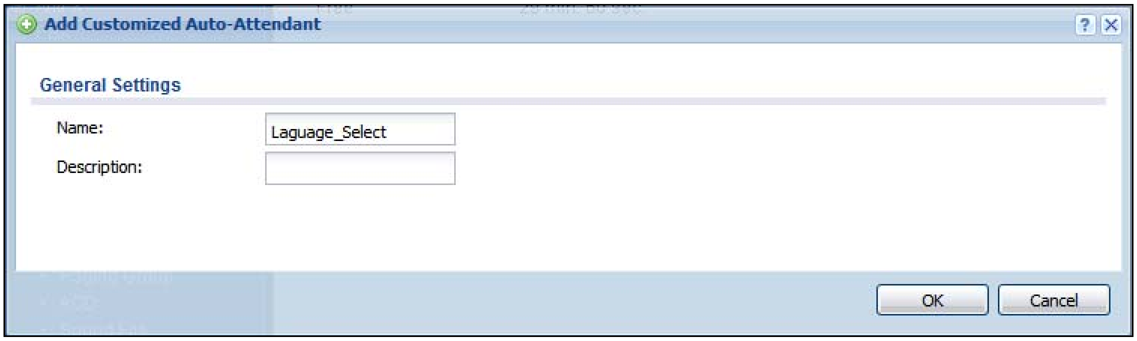
2 Click the **Add** button.


Outbound Line Group
Auto-Attendant
LCR
Default
Customized
Auto-Attendant Summary
Add
Edit
Remove
Download
Upload
#
Name
Description
Page 1 of 1
Show 50 items
No data to display
Audio File

Quota Usage: 0%
Total: 30 min.
Used: 0 min.
Free: 29 min. 60 sec.

Delete Audio File:
Unused
All

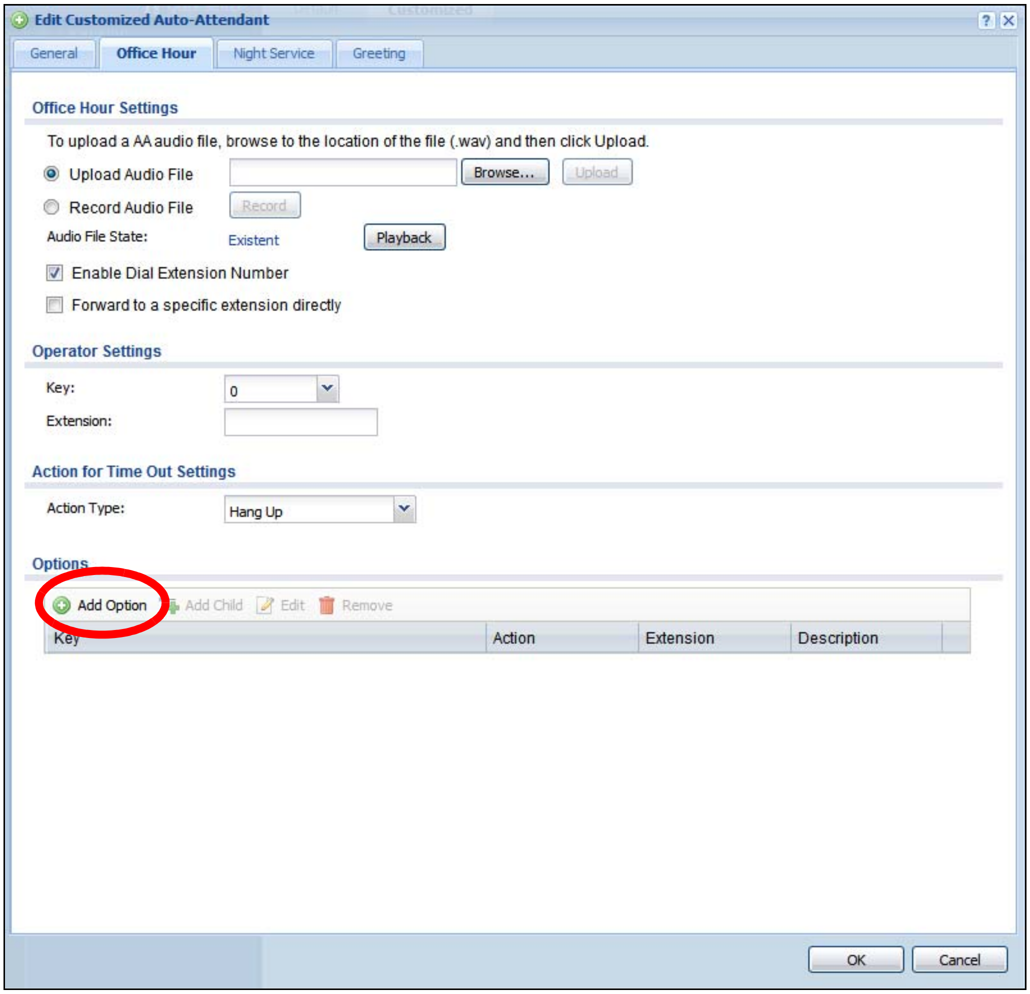
3 On the **Add Customized Auto-Attendant** screen, enter a **Name** and a **Description** (optional) for your first auto-attendant. The company manager of the Acme Widget company enters **Language_Select**, since this will be the first automated menu where callers choose either English or Spanish.


Add Customized Auto-Attendant
General Settings

Name: Laguage_Select
Description:

OK
Cancel

4 In the **Office Hour** tab provide an audio file saying something like “Press 1 for English or 2 for Spanish” to tell callers to select a language. Either upload an audio file (see Section 31.3.2 on page 509) or record one on the extension set as the recording peer (see Section 39.4 on page 571) and then click the **Add Option** button.


Edit Customized Auto-Attendant
General
Office Hour
Night Service
Greeting

Office Hour Settings

To upload a AA audio file, browse to the location of the file (.wav) and then click Upload.

● Upload Audio File
Browse...
Upload
○ Record Audio File
Record
Audio File State: Existent
Playback

☑ Enable Dial Extension Number

☐ Forward to a specific extension directly

Operator Settings

Key: 0

Extension:

Action for Time Out Settings

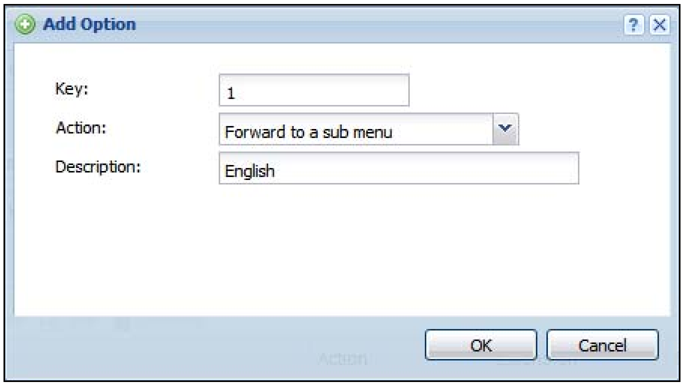
Action Type: Hang Up

Options

Add Option
Add Child
Edit
Remove

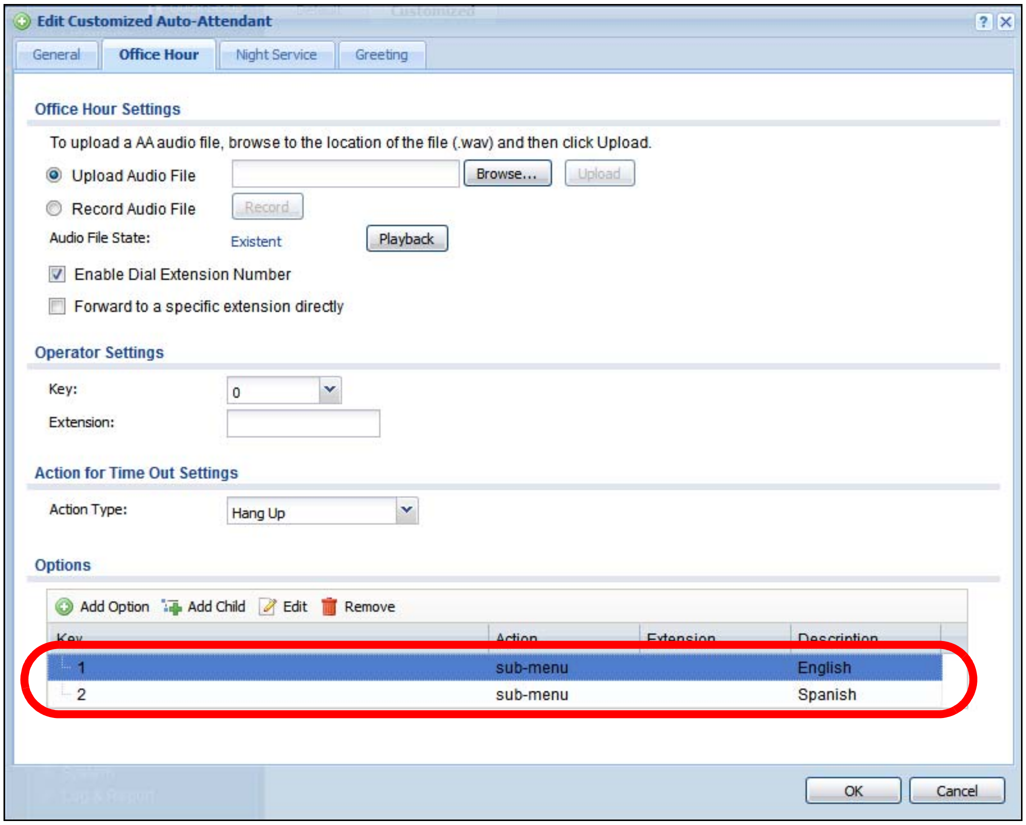
Key	Action	Extension	Description

5 In the **Add Option** screen, enter a keypad number and action for your auto-attendant. Because this is the language selection auto-attendant for the Acme Widget company, the company manager enters “1” for **Key**, “English” for **Description**, and selects “**Forward to a sub menu**” for **Action**. The action selected here is quite important because it allows us to open up the second tier submenu.


Add Option
OK
Cancel

Key: 1
Action: Forward to a sub menu
Description: English

6 Click **OK** to save these settings, then repeat this process for any other menu options (such as “Spanish” for the Acme Widget company).


Edit Customized Auto-Attendant
General
Office Hour
Night Service
Greeting
Office Hour Settings
Browse...
Upload
Record
Playback
Operator Settings
Action for Time Out Settings
Options
Add Option
Add Child
Edit
Remove
OK
Cancel

To upload a AA audio file, browse to the location of the file (.wav) and then click Upload.

● Upload Audio File
○ Record Audio File

Audio File State: Existent

☑ Enable Dial Extension Number
☐ Forward to a specific extension directly

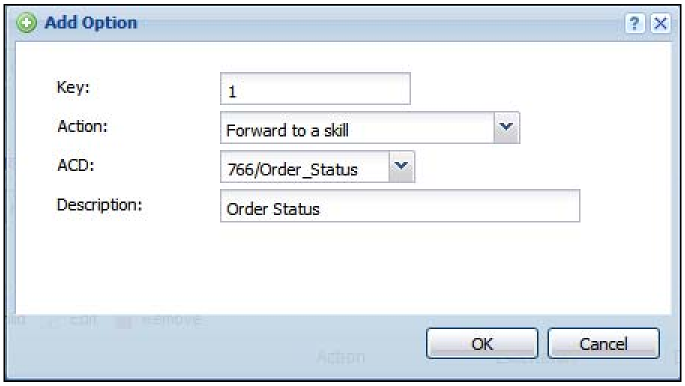
Key: 0
Extension:

Action Type: Hang Up

Key	Action	Extension	Description
1	sub-menu		English
2	sub-menu		Spanish

7 Select an option (1 for English in this example) and click the **Add Child** button to configure the option’s submenu to connect to a skill.

8 On the **Add Option** screen, enter the keypad number and action for the submenu item. The company manager for the Acme Widget company enters “1” for **Key**, selects “Forward to a skill” for **Action**, selects “766/Order Status” from the list of configured skills for the **ACD**, and enters “Order Status” for **Description**.



Key: 1
Action: Forward to a skill
ACD: 766/Order_Status
Description: Order Status

9 Click **OK** to save these settings, then repeat this process for any other menu options (such as “Technical Support” and “Accounts and Billing” for the Acme Widget company).

10 Repeat for the other submenus, such as the Spanish submenu for the Acme Widget company.

Congratulations! If you followed each of the steps described in this tutorial, then you should have the barebones structure of an automated menu system for your telephone network.

PART II

Technical Reference

9

Dashboard

9.1 Overview

Use the **Dashboard** screens to check status information about the ISG50.

9.1.1 What You Can Do in this Chapter

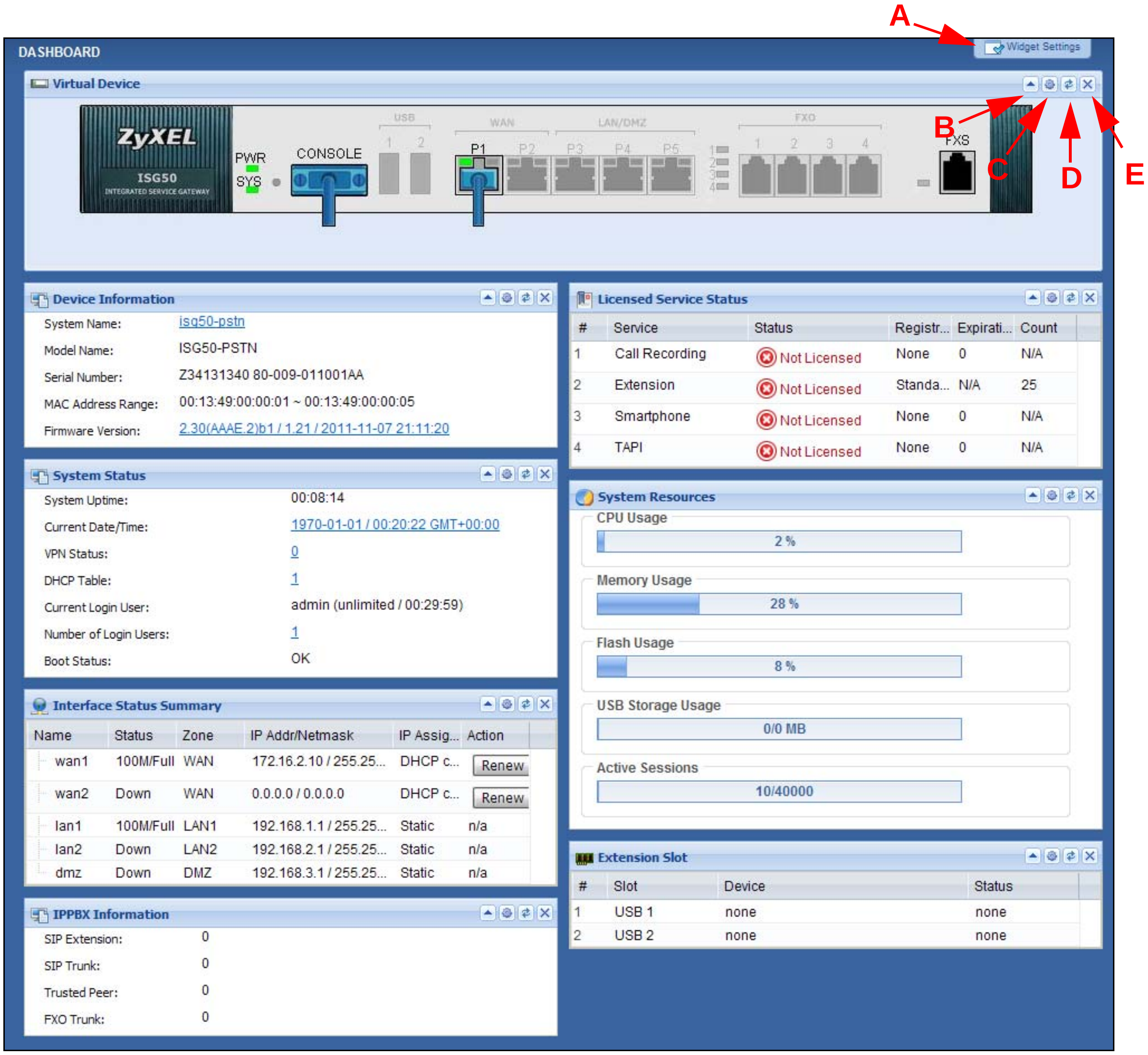
Use the **Dashboard** screens for the following.

- Use the main **Dashboard** screen (see Section 9.2 on page 185) to see the ISG50's general device information, system status, system resource usage, licensed service status, and interface status. You can also display other status screens for more information.
- Use the **VPN** status screen (see Section 9.2.1 on page 190) to look at the VPN tunnels that are currently established.
- Use the **DHCP Table** screen (see Section 9.2.5 on page 192) to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
- Use the **Current Users** screen (see Section 9.2.6 on page 193) to look at a list of the users currently logged into the ISG50.

9.2 The Dashboard Screen

The **Dashboard** screen displays when you log into the ISG50 or click **Dashboard** in the navigation panel. The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 135 Dashboard



Device Information

System Name: isg50-pstn
Model Name: ISG50-PSTN
Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:13:49:00:00:01 ~ 00:13:49:00:00:05
Firmware Version: 2.30(AAAE.2)b1 / 1.21 / 2011-11-07 21:11:20

System Status

System Uptime: 00:08:14
Current Date/Time: 1970-01-01 / 00:20:22 GMT+00:00
VPN Status: 0
DHCP Table: 1
Current Login User: admin (unlimited / 00:29:59)
Number of Login Users: 1
Boot Status: OK

Interface Status Summary

Name	Status	Zone	IP Addr/Netmask	IP Assig...	Action
wan1	100M/Full	WAN	172.16.2.10 / 255.25...	DHCP c...	Renew
wan2	Down	WAN	0.0.0.0 / 0.0.0.0	DHCP c...	Renew
lan1	100M/Full	LAN1	192.168.1.1 / 255.25...	Static	n/a
lan2	Down	LAN2	192.168.2.1 / 255.25...	Static	n/a
dmz	Down	DMZ	192.168.3.1 / 255.25...	Static	n/a

IPPBX Information

SIP Extension: 0
SIP Trunk: 0
Trusted Peer: 0
FXO Trunk: 0

Licensed Service Status

#	Service	Status	Registr...	Expirati...	Count
1	Call Recording	Not Licensed	None	0	N/A
2	Extension	Not Licensed	Standa...	N/A	25
3	Smartphone	Not Licensed	None	0	N/A
4	TAPI	Not Licensed	None	0	N/A

System Resources

CPU Usage: 2 %
Memory Usage: 28 %
Flash Usage: 8 %
USB Storage Usage: 0/0 MB
Active Sessions: 10/40000

Extension Slot

#	Slot	Device	Status
1	USB 1	none	none
2	USB 2	none	none

The following table describes the labels in this screen.

Table 26 Dashboard

LABEL	DESCRIPTION
Widget Settings (A)	Use this link to re-open closed widgets. Widgets that are already open appear grayed out.
Expand/collapse widget (B)	Click this to expand or collapse a widget.
Refresh time setting (C)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (D)	Click this to update the widget’s information immediately.
Close widget (E)	Click this to close the widget. Use **Widget Settings** to re-open it.

Table 26 Dashboard (continued)

LABEL	DESCRIPTION
Virtual Device	Hover your cursor over a LED, interface or slot to view details about the status of the ISG50 connections. See Section 1.4.1 on page 33 for LED descriptions. An unconnected interface or slot appears grayed out.
Device	This identifies a device installed in one of the ISG50's USB ports.
Name	The configuration name of the interface.
Status	This field displays the current status of each Ethernet interface. The possible values depend on what type of interface it is. For Ethernet interfaces: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (3G) interfaces, see Section 12.5 on page 251 for the status that can appear.
Zone	This field displays the zone to which the interface is currently assigned.
IP Address	This field displays the current IP address assigned to the interface.
Mask	This field displays the current subnet mask assigned to the interface.
1~4	**FXO**: **Off** - The port is not connected. **Blinking** - The line is ringing. **On** - A phone is plugged into the port and connected. **BRI**: **Off** - The port is not connected. **Blinking** - The port has at least one connection active. **On** - A phone is plugged into the port and connected.
FXS	**Off** - The port is not connected or on-hook **Blinking** - The phone is ringing for an inbound call. **On** - The port is off-hook.
Device Information	
System Name	This field displays the name used to identify the ISG50 on any network. Click the icon to open the screen where you can change it. See Section 52.2 on page 666.
Model Name	This field displays the model name of this ISG50.
Serial Number	This field displays the serial number of this ISG50.
MAC Address Range	This field displays the MAC addresses used by the ISG50. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on.
Firmware Version	This field displays the version number and date of the firmware the ISG50 is currently running. Click the icon to open the screen where you can upload firmware. See Section 55.3 on page 731.
System Status	
System Uptime	This field displays how long the ISG50 has been running since it last restarted or was turned on.

Table 26 Dashboard (continued)

LABEL	DESCRIPTION
Current Date/ Time	This field displays the current date and time in the ISG50. The format is yyyy-mm-dd hh:mm:ss.
VPN Status	Click this to look at the VPN tunnels that are currently established. See Section 9.2.1 on page 190.
DHCP Table	Click this to look at the IP addresses currently assigned to the ISG50's DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 9.2.5 on page 192.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining. See Chapter 44 on page 599.
Number of Login Users	This field displays the number of users currently logged in to the ISG50. Click the icon to pop-open a list of the users who are currently logged in to the ISG50. See Section 9.2.6 on page 193.
Boot Status	This field displays details about the ISG50's startup state. **OK** - The ISG50 started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - The ISG50 successfully applied the system default configuration. This occurs when the ISG50 starts for the first time or you intentionally reset the ISG50 to the system default settings. **Fallback to lastgood configuration** - The ISG50 was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The ISG50 was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The ISG50 is still applying the system configuration.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (3G) interfaces, see Section 10.10 on page 210 for the status that can appear.
Zone	This field displays the zone to which the interface is currently assigned.
IP Addr/ Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.
IP Assignment	This shows whether the interface gets an IP address automatically (**DHCP**) or has a fixed IP address (**Static**).

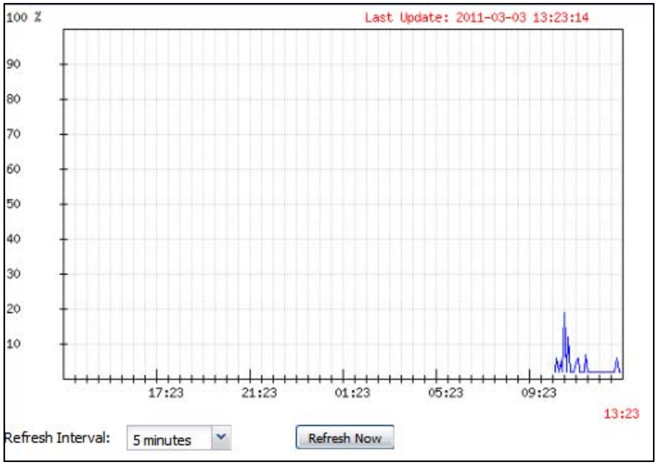
Table 26 Dashboard (continued)

LABEL	DESCRIPTION
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click the **Connect** icon to have the ISG50 try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**. Click the **Disconnect** icon to stop a PPPoE/PPTP connection.
IPPBX Information	
SIP Extension	This shows the number of SIP extensions currently configured in the ISG50.
SIP Trunk	This shows the number of SIP trunks currently configured in the ISG50.
Trust Peer	This shows the number of trusted peers currently configured in the ISG50.
FXO Trunk	This shows the number of FXO trunks currently configured in the ISG50.
BRI Trunk	This shows the number of BRI trunks currently configured in the ISG50.
Licensed Service Status	
#	This shows how many licensed services there are. Individual index numbers are not associated with specific services.
Service	This is the name of the licensed service.
Status	This is the current status of the license.
Registration	This is the type of registration required to use the licensed service.
Expiration date	If the service license is valid, this shows when it will expire. N/A displays if the service license does not have a limited period of validity.
Count	This shows how many units the licensed service permits.
System Resources	
CPU Usage	This field displays what percentage of the ISG50's processing capability is currently being used. Hover your cursor over this field to display the **Show CPU Usage** icon that takes you to a chart of the ISG50's recent CPU usage.
Memory Usage	This field displays what percentage of the ISG50's RAM is currently being used. Hover your cursor over this field to display the **Show Memory Usage** icon that takes you to a chart of the ISG50's recent memory usage.
Flash Usage	This field displays what percentage of the ISG50's onboard flash memory is currently being used.
USB Storage Usage	This field displays how much of the ISG50's connected USB storage is currently being used.
Active Sessions	This field displays how many traffic sessions are currently open on the ISG50. These are the sessions that are traversing the ISG50. Hover your cursor over this field to display icons. Click the **Detail** icon to go to the **Session Monitor** screen to see details about the active sessions. Click the **Show Active Sessions** icon to display a chart of ISG50's recent session usage.
Extension Slot	This section of the screen displays the status of the USB ports.
#	This field displays how many USB ports there are.
Slot	This field displays the name of each extension slot.
Device	This field displays the name of the device connected to the USB port (or **none** if no device is detected).
Status	For cellular (3G) interfaces, see Section 10.10 on page 210 for the status that can appear.

9.2.1 The CPU Usage Screen

Use this screen to look at a chart of the ISG50's recent CPU usage. To access this screen, click **Show CPU Usage** in the dashboard.

Figure 136 Dashboard > Show CPU Usage



Last Update: 2011-03-03 13:23:14

Refresh Interval: 5 minutes

100 %
90
80
70
60
50
40
30
20
10
17:23
21:23
01:23
05:23
09:23
13:23
Refresh Now

The following table describes the labels in this screen.

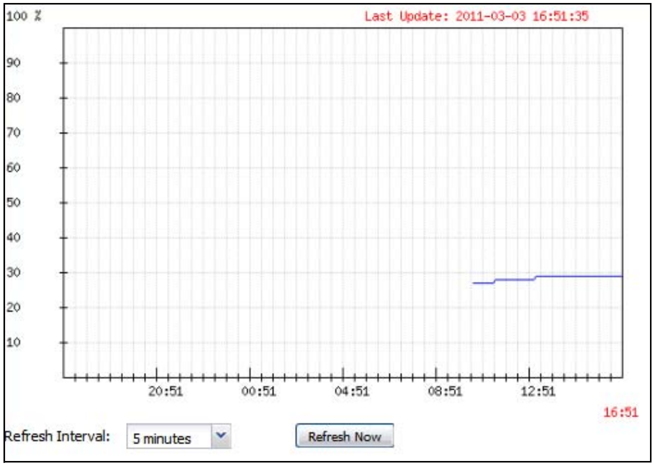
Table 27 Dashboard > Show CPU Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of CPU usage.
	The x-axis shows the time period over which the CPU usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

9.2.2 The Memory Usage Screen

Use this screen to look at a chart of the ISG50's recent memory (RAM) usage. To access this screen, click **Show Memory Usage** in the dashboard.

Figure 137 Dashboard > Show Memory Usage



Last Update: 2011-03-03 16:51:35

Refresh Interval: 5 minutes

100 %
90
80
70
60
50
40
30
20
10
20:51
00:51
04:51
08:51
12:51
16:51
Refresh Now

The following table describes the labels in this screen.

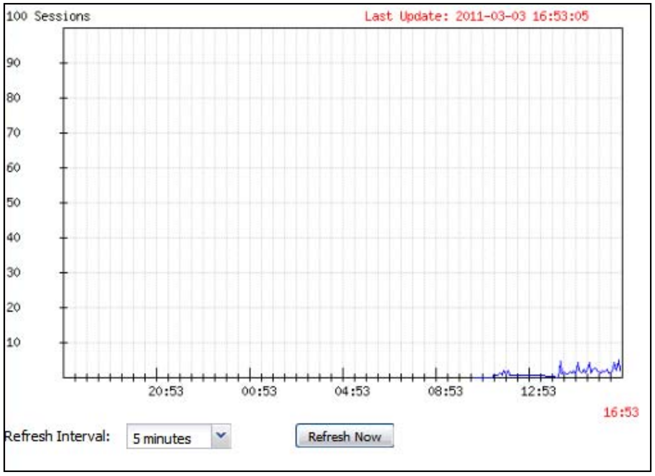
Table 28 Dashboard > Show Memory Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of RAM usage.
	The x-axis shows the time period over which the RAM usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

9.2.3 The Active Sessions Screen

Use this screen to look at a chart of the ISG50's recent traffic session usage. To access this screen, click **Show Active Sessions** in the dashboard.

Figure 138 Dashboard > Show Active Sessions



Refresh Interval: 5 minutes

The following table describes the labels in this screen.

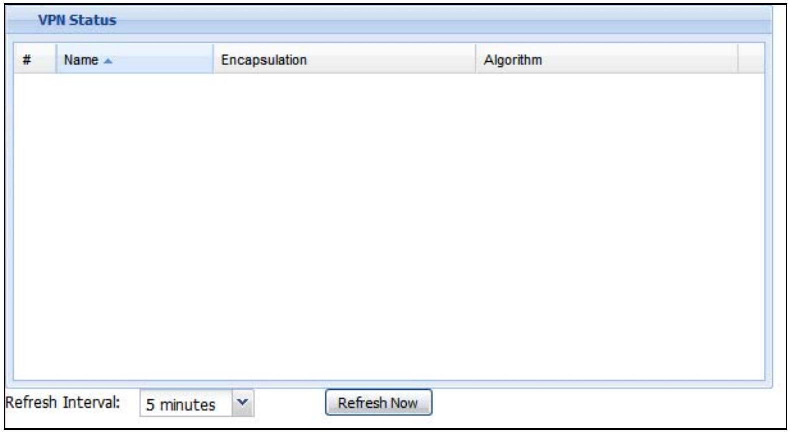
Table 29 Dashboard > Show Active Sessions

LABEL	DESCRIPTION
Sessions	The y-axis represents the number of session.
	The x-axis shows the time period over which the session usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

9.2.4 The VPN Status Screen

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **VPN Status** in the dashboard.

Figure 139 Dashboard > VPN Status


VPN Status
#
Name
Encapsulation
Algorithm
Refresh Interval:
5 minutes
Refresh Now

The following table describes the labels in this screen.

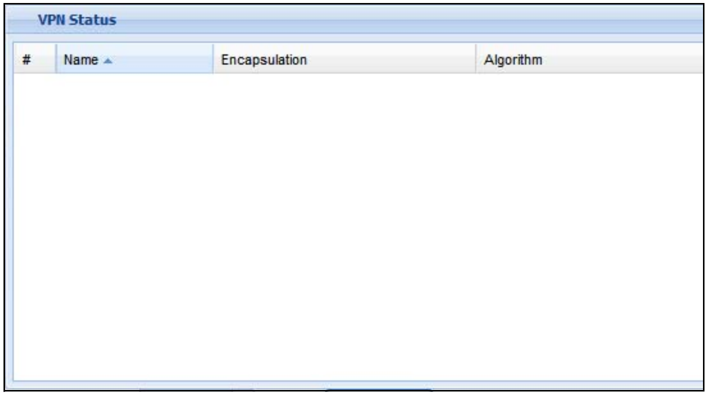
Table 30 Dashboard > VPN Status

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Refresh Interval	Select how often you want this window to be updated automatically.
Refresh Now	Click this to update the information in the window right away.

9.2.5 The DHCP Table Screen

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. To access this screen, click **DHCP Table** in the dashboard.

Figure 140 Dashboard > DHCP Table


VPN Status
#
Name
Encapsulation
Algorithm

The following table describes the labels in this screen.

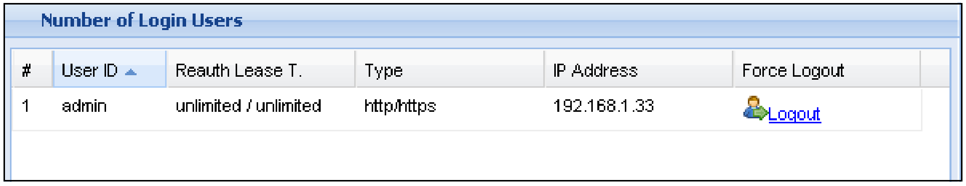
Table 31 Dashboard > DHCP Table

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Interface	This field identifies the interface that assigned an IP address to a DHCP client.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order.
Host Name	This field displays the name used to identify this device on the network (the computer name). The ISG50 learns these from the DHCP client requests. "None" shows here for a static DHCP entry.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. Click the column's heading cell to sort the table entries by MAC address. Click the heading cell again to reverse the sort order.
Description	For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries.
Reserve	If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address. If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client. To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click **Apply**. To remove a static DHCP entry, clear this field, and then click **Apply**.
Refresh Interval	Select how often you want this window to be updated automatically.
Refresh Now	Click this to update the information in the window right away.

9.2.6 The Number of Login Users Screen

Use this screen to look at a list of the users currently logged into the ISG50. To access this screen, click the dashboard's **Number of Login Users** icon.

Figure 141 Dashboard > Number of Login Users



Number of Login Users

#	User ID	Reauth Lease T.	Type	IP Address	Force Logout
1	admin	unlimited / unlimited	http/https	192.168.1.33	Logout

The following table describes the labels in this screen.

Table 32 Dashboard > Number of Login Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the ISG50.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 44 on page 599.
Type	This field displays the way the user logged in to the ISG50.

Table 32 Dashboard > Number of Login Users (continued)

LABEL	DESCRIPTION
IP address	This field displays the IP address of the computer used to log in to the ISG50.
Force Logout	Click this icon to end a user’s session.

10

Monitor

10.1 Overview

Use the **Monitor** screens to check status and statistics information.

10.1.1 What You Can Do in this Chapter

Use the **Monitor** screens for the following.

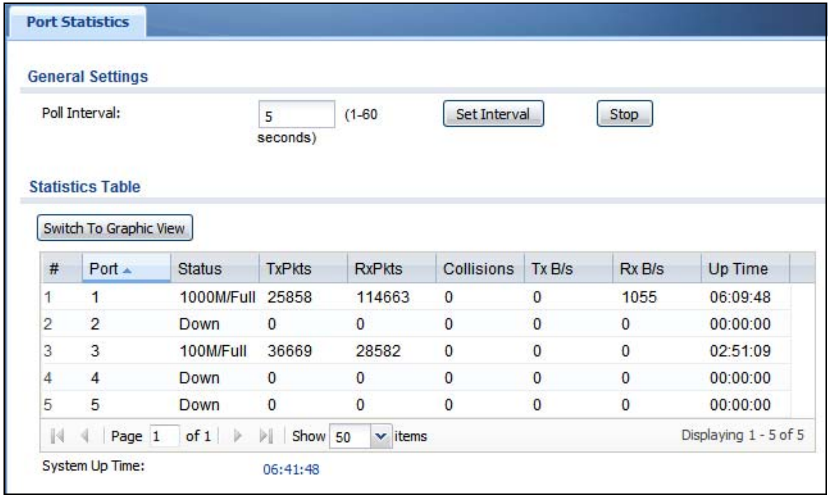
- Use the **System Status > Port Statistics** screen (see Section 10.2 on page 196) to look at packet statistics for each physical port.
- Use the **System Status > Port Statistics > Graph View** screen (see Section 10.2 on page 196) to look at a line graph of packet statistics for each physical port.
- Use the **System Status > Interface Status** screen (Section 10.3 on page 198) to see all of the ISG50's interfaces and their packet statistics.
- Use the **System Status > Traffic Statistics** screen (see Section 10.4 on page 200) to start or stop data collection and view statistics.
- Use the **System Status > Session Monitor** screen (see Section 10.5 on page 203) to view sessions by user or service.
- Use the **System Status > DDNS Status** screen (see Section 10.6 on page 205) to view the status of the ISG50's DDNS domain names.
- Use the **System Status > IP/MAC Binding** screen (Section 10.7 on page 205) to view a list of devices that have received an IP address from ISG50 interfaces with IP/MAC binding enabled.
- Use the **System Status > Login Users** screen (Section 10.8 on page 206) to look at a list of the users currently logged into the ISG50.
- Use the **System Status > Cellular Status** screen (Section 10.9 on page 207) to check your 3G connection status.
- Use the **System Status > USB Storage** screen (Section 10.10 on page 210) to view information about a connected USB storage device.
- Use the **VPN Monitor** > **IPSec** screen (Section 10.11 on page 211) to display and manage active IPSec SAs.
- Use the **PBX > SIP Peer** screen (Section 10.12 on page 213) to display information about the ISG50's SIP extensions.
- Use the **PBX > FXS Peer** screen (Section 10.13 on page 214) to display information about the ISG50's FXS extensions.
- Use the **PBX > SIP Trunk** screen (Section 10.14 on page 215) to display status information about external connections to other SIP servers.
- Use the **PBX > CTI Peer** screen (Section 10.15 on page 216) to display status information about the ISG50's Computer Telephony Integration (CTI) connections.
- Use the **PBX > FXO Trunk** screen (Section 10.16 on page 217) to display status information about external connections via FXO interfaces.

- Use the **PBX > BRI Trunk** screen (Section 10.17 on page 218) to display status information about external connections via BRI interfaces.
- Use the **PBX > ACD Queue** screen (Section 10.18 on page 219) to monitor phone call activity for Automatic Call Distribution (ACD) agents.
- Use the **System Log** screen (Section 10.19 on page 220) to view the ISG50's current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.
- Use the **Call Recording** screen (Section 10.20 on page 222) to search for call recordings on the ISG50.
- Use the **CDR** screens (Section 10.21 on page 223 to Section 10.23 on page 227) to backup or search for call records on the ISG50.

10.2 The Port Statistics Screen

Use this screen to look at packet statistics for each Gigabit Ethernet port. To access this screen, click **Monitor > System Status** > **Port Statistics**.

Figure 142 Monitor > System Status > Port Statistics



Poll Interval: 5 (1-60 seconds)

#	Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
1	1	1000M/Full	25858	114663	0	0	1055	06:09:48
2	2	Down	0	0	0	0	0	00:00:00
3	3	100M/Full	36669	28582	0	0	0	02:51:09
4	4	Down	0	0	0	0	0	00:00:00
5	5	Down	0	0	0	0	0	00:00:00

Page 1 of 1 | Show 50 items | Displaying 1 - 5 of 5

System Up Time: 06:41:48

The following table describes the labels in this screen.

Table 33 Monitor > System Status > Port Statistics

LABEL	DESCRIPTION
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.
Switch to Graphic View	Click this to display the port statistics as a line graph.
#	This field displays the port's number in the list.
Port	This field displays the physical port number.

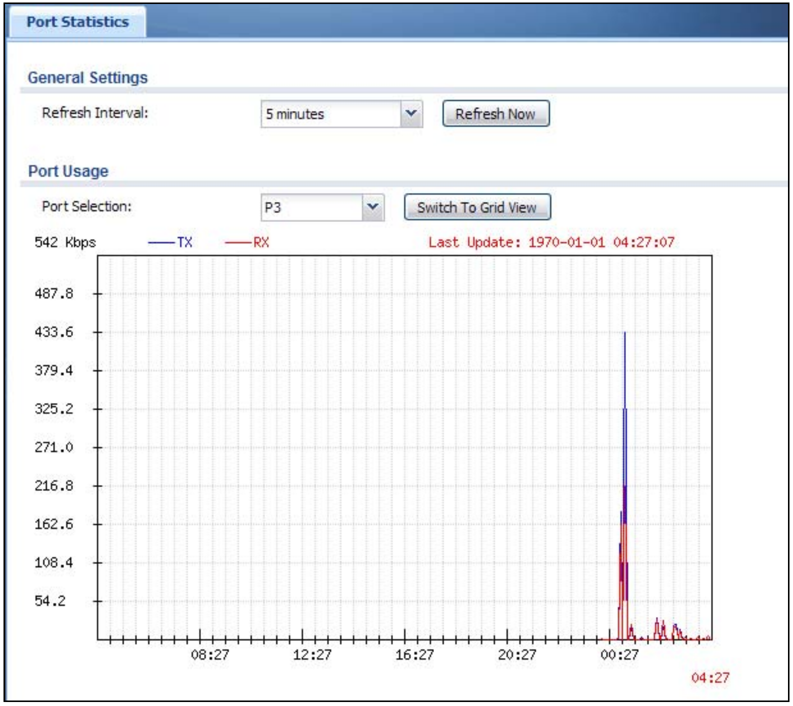
Table 33 Monitor > System Status > Port Statistics (continued)

LABEL	DESCRIPTION
Status	This field displays the current status of the physical port. **Down** - The physical port is not connected. **Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the ISG50 on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the ISG50 on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.

10.2.1 The Port Statistics Graph Screen

Use this screen to look at a line graph of packet statistics for each physical port. To access this screen, click **Port Statistics** in the **Status** screen and then the **Switch to Graphic View Button**.

Figure 143 Monitor > System Status > Port Statistics > Switch to Graphic View



Refresh Interval: 5 minutes

Port Selection: P3

Last Update: 1970-01-01 04:27:07

Port Statistics
General Settings
Refresh Now
Port Usage
Switch To Grid View
542 Kbps
TX
RX
487.8
433.6
379.4
325.2
271.0
216.8
162.6
108.4
54.2
08:27
12:27
16:27
20:27
00:27
04:27

The following table describes the labels in this screen.

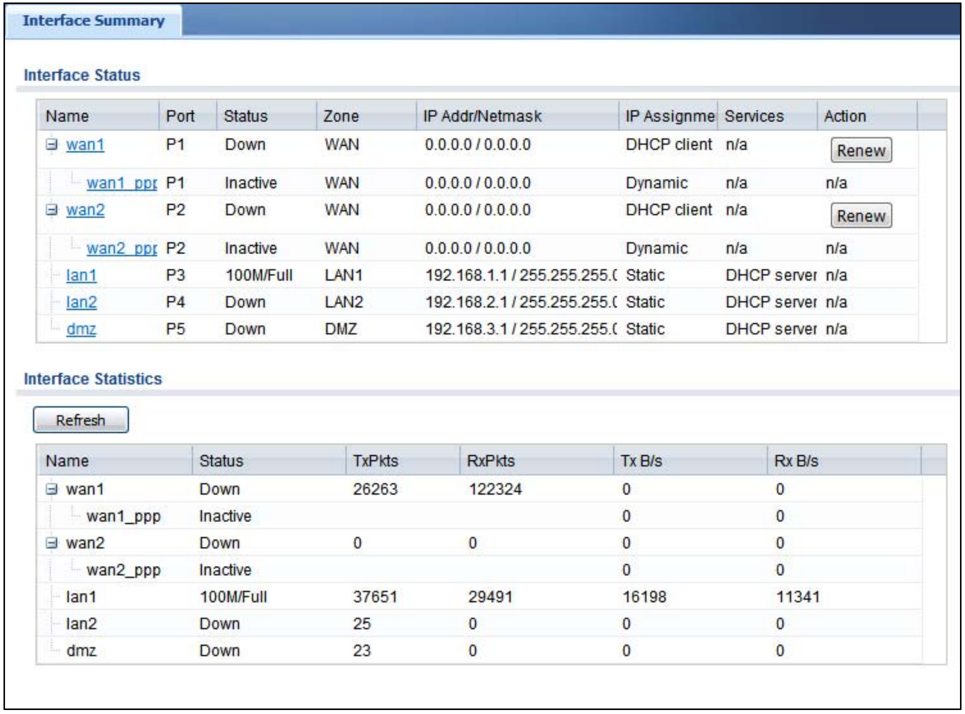
Table 34 Monitor > System Status > Port Statistics > Switch to Graphic View

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Selection	Select the number of the physical port for which you want to display graphics.
Switch to Grid View	Click this to display the port statistics as a table.
bps	The y-axis represents the speed of transmission or reception.
time	The x-axis shows the time period over which the transmission or reception occurred
TX	This line represents traffic transmitted from the ISG50 on the physical port since it was last connected.
RX	This line represents the traffic received by the ISG50 on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.

10.3 Interface Status Screen

This screen lists all of the ISG50’s interfaces and gives packet statistics for them. Click **Monitor > System Status > Interface Status** to access this screen.

Figure 144 Monitor > System Status > Interface Status



Interface Status

Name	Port	Status	Zone	IP Addr/Netmask	IP Assignme	Services	Action
⊟ wan1	P1	Down	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan1_pp	P1	Inactive	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
⊟ wan2	P2	Down	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_pp	P2	Inactive	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P3	100M/Full	LAN1	192.168.1.1 / 255.255.255.	Static	DHCP serve	n/a
lan2	P4	Down	LAN2	192.168.2.1 / 255.255.255.	Static	DHCP serve	n/a
dmz	P5	Down	DMZ	192.168.3.1 / 255.255.255.	Static	DHCP serve	n/a

Interface Statistics

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
⊟ wan1	Down	26263	122324	0	0
wan1_ppp	Inactive			0	0
⊟ wan2	Down	0	0	0	0
wan2_ppp	Inactive			0	0
lan1	100M/Full	37651	29491	16198	11341
lan2	Down	25	0	0	0
dmz	Down	23	0	0	0

Each field is described in the following table.

Table 35 Monitor > System Status > Interface Status

LABEL	DESCRIPTION
Interface Status	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.
Name	This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface.
Port	This field displays the physical port number.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (3G) interfaces, see Section 10.10 on page 210 for the status that can appear. For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPP interfaces: **Connected** - The PPP interface is connected. **Disconnected** - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list.
Zone	This field displays the zone to which the interface is assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.
Services	This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. This field displays **n/a** if the interface does not provide any services to the network.
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click **Connect** to try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.
Interface Statistics	This table provides packet statistics for each interface.
Refresh	Click this button to update the information in the screen.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.

Table 35 Monitor > System Status > Interface Status (continued)

LABEL	DESCRIPTION
Name	This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the statistics for virtual interfaces on top of this interface.
Status	This field displays the current status of the interface. **Down** - The interface is not connected. **Speed / Duplex** - The interface is connected. This field displays the port speed and duplex setting (**Full** or **Half**). This field displays **Connected** and the accumulated connection time (hh:mm:ss) when the PPP interface is connected.
TxPkts	This field displays the number of packets transmitted from the ISG50 on the interface since it was last connected.
RxPkts	This field displays the number of packets received by the ISG50 on the interface since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated.

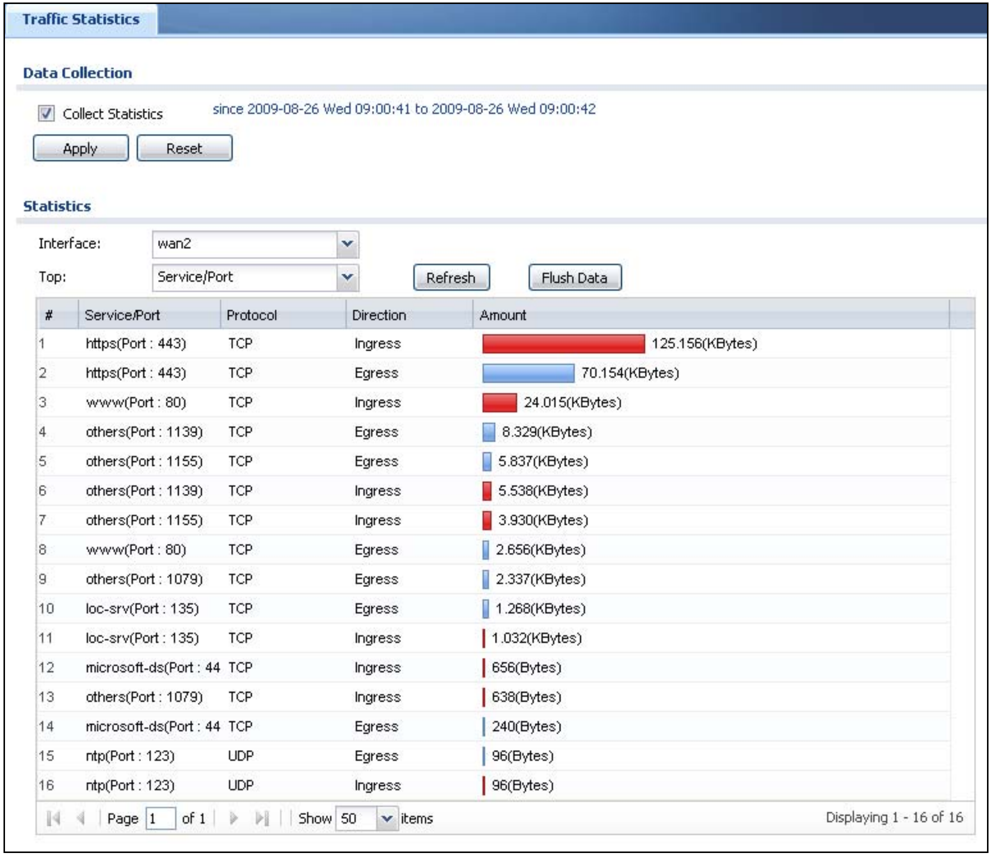
10.4 The Traffic Statistics Screen

Click **Monitor > System Status > Traffic Statistics** to display the **Traffic Statistics** screen. This screen provides basic information about the following for example:

- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the ISG50 counts HTTP GET packets. Please see Table 36 on page 201 for more information.
- Most-used protocols or service ports and the amount of traffic on each one
- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

You use the **Traffic Statistics** screen to tell the ISG50 when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the **Traffic Statistics** screen.

Figure 145 Monitor > System Status > Traffic Statistics



☑ Collect Statistics since 2009-08-26 Wed 09:00:41 to 2009-08-26 Wed 09:00:42

Interface: wan2

Top: Service/Port

#	Service/Port	Protocol	Direction	Amount
1	https(Port : 443)	TCP	Ingress	125.156(KBytes)
2	https(Port : 443)	TCP	Egress	70.154(KBytes)
3	www(Port : 80)	TCP	Ingress	24.015(KBytes)
4	others(Port : 1139)	TCP	Egress	8.329(KBytes)
5	others(Port : 1155)	TCP	Egress	5.837(KBytes)
6	others(Port : 1139)	TCP	Ingress	5.538(KBytes)
7	others(Port : 1155)	TCP	Ingress	3.930(KBytes)
8	www(Port : 80)	TCP	Egress	2.656(KBytes)
9	others(Port : 1079)	TCP	Egress	2.337(KBytes)
10	loc-srv(Port : 135)	TCP	Egress	1.268(KBytes)
11	loc-srv(Port : 135)	TCP	Ingress	1.032(KBytes)
12	microsoft-ds(Port : 44	TCP	Ingress	656(Bytes)
13	others(Port : 1079)	TCP	Ingress	638(Bytes)
14	microsoft-ds(Port : 44	TCP	Egress	240(Bytes)
15	ntp(Port : 123)	UDP	Egress	96(Bytes)
16	ntp(Port : 123)	UDP	Ingress	96(Bytes)

Page 1 of 1 | Show 50 items | Displaying 1 - 16 of 16

There is a limit on the number of records shown in the report. Please see Table 37 on page 203 for more information. The following table describes the labels in this screen.

Table 36 Monitor > System Status > Traffic Statistics

LABEL	DESCRIPTION
Data Collection	
Collect Statistics	Select this to have the ISG50 collect data for the report. If the ISG50 has already been collecting data, the collection period displays to the right. The progress is not tracked here real-time, but you can click the **Refresh** button to update it.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.
Statistics	
Interface	Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge and PPPoE/PPTP interfaces.

Table 36 Monitor > System Status > Traffic Statistics (continued)

LABEL	DESCRIPTION
Top	Select the type of report to display. Choices are: **Host IP Address/User** - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one. **Service/Port** - displays the most-used protocols or service ports and the amount of traffic for each one. **Web Site Hits** - displays the most-visited Web sites and how many times each one has been visited. Each type of report has different information in the report (below).
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
	These fields are available when the **Traffic Type** is **Host IP Address/User**.
#	This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic.
IP Address/User	This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 37 on page 203.
Direction	This field indicates whether the IP address or user is sending or receiving traffic. **Ingress**- traffic is coming from the IP address or user to the ISG50. **Egress** - traffic is going from the ISG50 to the IP address or user.
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. If the **Direction** is **Ingress**, a red bar is displayed; if the **Direction** is **Egress**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 37 on page 203.
	These fields are available when the **Traffic Type** is **Service/Port**.
#	This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic.
Service/Port	This field displays the service and port in this record. The maximum number of services and service ports in this report is indicated in Table 37 on page 203.
Protocol	This field indicates what protocol the service was using.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. **Ingress** - traffic is coming into the router through the interface **Egress** - traffic is going out from the router through the interface
Amount	This field displays how much traffic was sent or received from the indicated service / port. If the **Direction** is **Ingress**, a red bar is displayed; if the **Direction** is **Egress**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 37 on page 203.
	These fields are available when the **Traffic Type** is **Web Site Hits**.
#	This field is the rank of each record. The domain names are sorted by the number of hits.
Web Site	This field displays the domain names most often visited. The ISG50 counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 37 on page 203.
Hits	This field displays how many hits the Web site received. The ISG50 counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the ISG50 counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 37 on page 203.

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

Table 37 Maximum Values for Reports

LABEL	DESCRIPTION
Maximum Number of Records	20
Byte Count Limit	2^{64} bytes; this is just less than 17 million terabytes.
Hit Count Limit	2^{64} hits; this is over 1.8 x 10^{19} hits.

10.5 The Session Monitor Screen

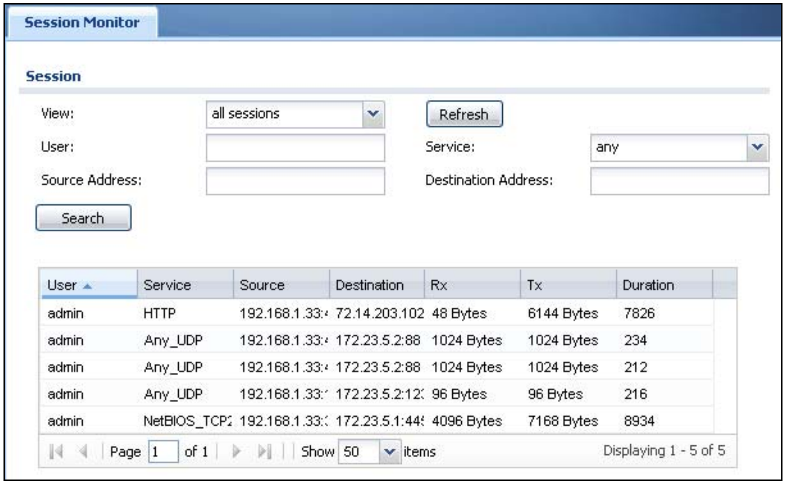
The **Session Monitor** screen displays information about active sessions for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all the active sessions by user, service, source IP address, or destination IP address. You can also filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

Click **Monitor > System Status > Session Monitor** to display the following screen.

Figure 146 Monitor > System Status > Session Monitor



View: all sessions

Service: any

User	Service	Source	Destination	Rx	Tx	Duration
admin	HTTP	192.168.1.33:	72.14.203.102	48 Bytes	6144 Bytes	7826
admin	Any_UDP	192.168.1.33:	172.23.5.2:88	1024 Bytes	1024 Bytes	234
admin	Any_UDP	192.168.1.33:	172.23.5.2:88	1024 Bytes	1024 Bytes	212
admin	Any_UDP	192.168.1.33:	172.23.5.2:12	96 Bytes	96 Bytes	216
admin	NetBIOS_TCP	192.168.1.33:	172.23.5.1:44	4096 Bytes	7168 Bytes	8934

The following table describes the labels in this screen.

Table 38 Monitor > System Status > Session Monitor

LABEL	DESCRIPTION
View	Select how you want the information to be displayed. Choices are: **sessions by users** - display all active sessions grouped by user **sessions by services** - display all active sessions grouped by service or protocol **sessions by source IP** - display all active sessions grouped by source IP address **sessions by destination IP** - display all active sessions grouped by destination IP address **all sessions** - filter the active sessions by the **User**, **Service**, **Source Address**, and **Destination Address**, and display each session individually (sorted by user).
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
	The **User**, **Service**, **Source Address**, and **Destination Address** fields display if you view all sessions. Select your desired filter criteria and click the **Search** button to filter the list of sessions.
User	This field displays when **View** is set to **all sessions**. Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name.
Service	This field displays when **View** is set to **all sessions**. Select the service or service group whose sessions you want to view. The ISG50 identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined. (See Chapter 46 on page 619 for more information about services.)
Source Address	This field displays when **View** is set to **all sessions**. Type the source IP address whose sessions you want to view. You cannot include the source port.
Destination Address	This field displays when **View** is set to **all sessions**. Type the destination IP address whose sessions you want to view. You cannot include the destination port.
Search	This button displays when **View** is set to **all sessions**. Click this button to update the information on the screen using the filter criteria in the **User**, **Service**, **Source Address**, and **Destination Address** fields.
Active Sessions	This is the total number of active sessions that matched the search criteria.
Show	Select the number of active sessions displayed on each page. You can use the arrow keys on the right to change pages.
User	This field displays the user in each active session. If you are looking at the **sessions by users** (or **all sessions**) report, click **+** or **-** to display or hide details about a user's sessions.
Service	This field displays the protocol used in each active session. If you are looking at the **sessions by services** report, click **+** or **-** to display or hide details about a protocol's sessions.
Source	This field displays the source IP address and port in each active session. If you are looking at the **sessions by source IP** report, click **+** or **-** to display or hide details about a source IP address's sessions.
Destination	This field displays the destination IP address and port in each active session. If you are looking at the **sessions by destination IP** report, click **+** or **-** to display or hide details about a destination IP address's sessions.
Rx	This field displays the amount of information received by the source in the active session.

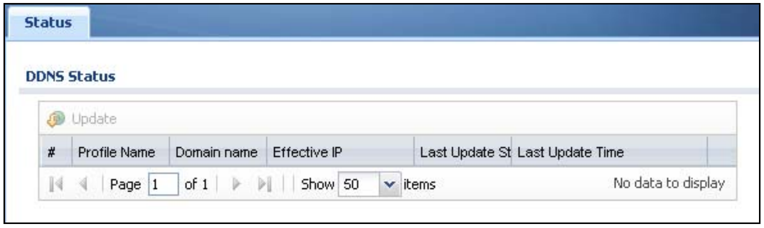
Table 38 Monitor > System Status > Session Monitor (continued)

LABEL	DESCRIPTION
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.

10.6 The DDNS Status Screen

The **DDNS Status** screen shows the status of the ISG50's DDNS domain names. Click **Monitor > System Status > DDNS Status** to open the following screen.

Figure 147 Monitor > System Status > DDNS Status



The following table describes the labels in this screen.

Table 39 Monitor > System Status > DDNS Status

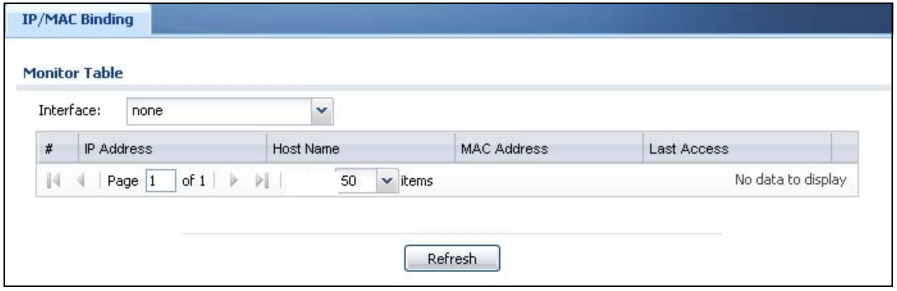
LABEL	DESCRIPTION
Update	Click this to have the ISG50 update the profile to the DDNS server. The ISG50 attempts to resolve the IP address for the domain name.
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the ISG50 can route.
Effective IP	This is the (resolved) IP address of the domain name.
Last Update Status	This shows whether the last attempt to resolve the IP address for the domain name was successful or not. **Updating** means the ISG50 is currently attempting to resolve the IP address for the domain name.
Last Update Time	This shows when the last attempt to resolve the IP address for the domain name occurred (in year-month-day hour:minute:second format).

10.7 IP/MAC Binding Monitor

Click **Monitor > System Status > IP/MAC Binding** to open the **IP/MAC Binding Monitor** screen. This screen lists the devices that have received an IP address from ISG50 interfaces with

IP/MAC binding enabled and have ever established a session with the ISG50. Devices that have never established a session with the ISG50 do not display in the list.

Figure 148 Monitor > System Status > IP/MAC Binding


IP/MAC Binding
Monitor Table
Page 1 of 1
50 items
No data to display
Refresh

Interface: none

#	IP Address	Host Name	MAC Address	Last Access

The following table describes the labels in this screen.

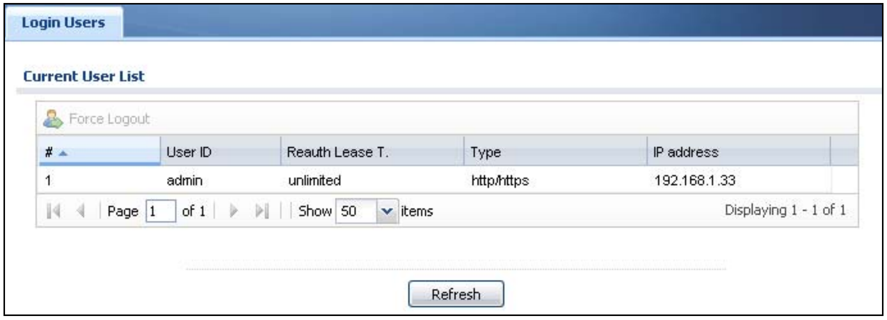
Table 40 Monitor > System Status > IP/MAC Binding

LABEL	DESCRIPTION
Interface	Select a ISG50 interface that has IP/MAC binding enabled to show to which devices it has assigned an IP address.
#	This is the index number of an IP/MAC binding entry.
IP Address	This is the IP address that the ISG50 assigned to a device.
Host Name	This field displays the name used to identify this device on the network (the computer name). The ISG50 learns these from the DHCP client requests.
MAC Address	This field displays the MAC address to which the IP address is currently assigned.
Last Access	This is when the device last established a session with the ISG50 through this interface.
Refresh	Click this button to update the information in the screen.

10.8 The Login Users Screen

Use this screen to look at a list of the users currently logged into the ISG50. To access this screen, click **Monitor > System Status > Login Users**.

Figure 149 Monitor > System Status > Login Users


Login Users
Current User List
Force Logout
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Refresh

#	User ID	Reauth Lease T.	Type	IP address
1	admin	unlimited	http/https	192.168.1.33

The following table describes the labels in this screen.

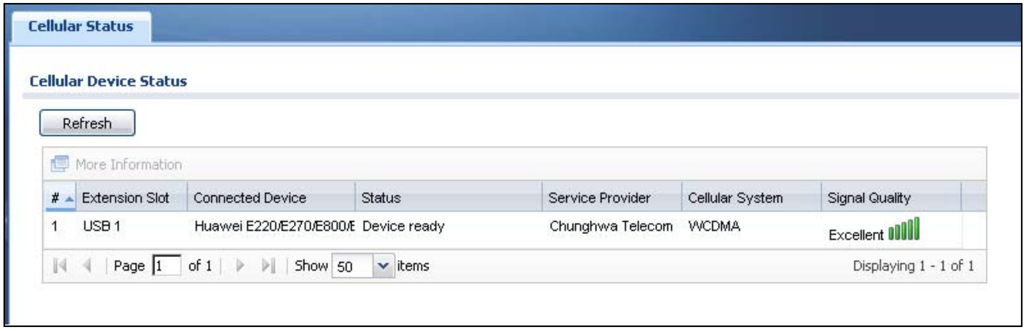
Table 41 Monitor > System Status > Login Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the ISG50.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 44 on page 599.
Type	This field displays the way the user logged in to the ISG50.
IP address	This field displays the IP address of the computer used to log in to the ISG50.
Force Logout	Click this icon to end a user’s session.
Refresh	Click this button to update the information in the screen.

10.9 Cellular Status Screen

This screen displays your 3G connection status. click **Monitor > System Status > Cellular Status** to display this screen.

Figure 150 Monitor > System Status > Cellular Status



#	Extension Slot	Connected Device	Status	Service Provider	Cellular System	Signal Quality
1	USB 1	Huawei E220/E270/E800/E	Device ready	Chunghwa Telecom	WCDMA	Excellent

The following table describes the labels in this screen.

Table 42 Monitor > System Status > Cellular Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information in the screen.
More Information	Click this to display more information on your 3G, such as the signal strength, IMEA/ESN and IMSI. This is only available when the 3G device attached and activated on your ISG50. Refer to Section 10.9.1 on page 209.
#	This field is a sequential value, and it is not associated with any interface.
Extension Slot	This field displays where the entry’s cellular card is located.
Connected Device	This field displays the model name of the cellular card.

Table 42 Monitor > System Status > Cellular Status (continued)

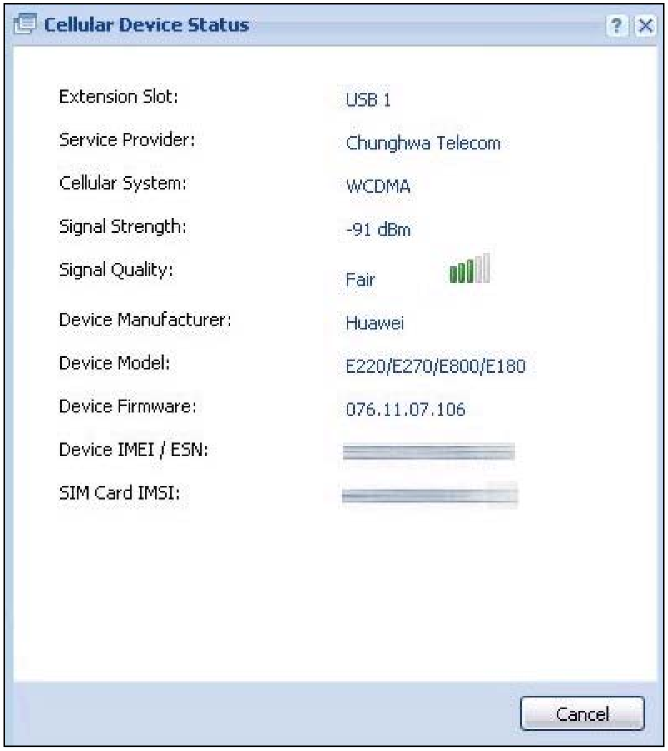
LABEL	DESCRIPTION
Status	**No device** - no 3G device is connected to the ISG50. **No Service** - no 3G network is available in the area; you cannot connect to the Internet. **Limited Service** - returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet. **Device detected** - displays when you connect a 3G device. **Device error** - a 3G device is connected but there is an error. **Probe device fail** - the ISG50's test of the 3G device failed. **Probe device ok** - the ISG50's test of the 3G device succeeded. **Init device fail** - the ISG50 was not able to initialize the 3G device. **Init device ok** - the ISG50 initialized the 3G card. **Check lock fail** - the ISG50's check of whether or not the 3G device is locked failed. **Device locked** - the 3G device is locked. **SIM error** - there is a SIM card error on the 3G device. **SIM locked-PUK** - the PUK is locked on the 3G device's SIM card. **SIM locked-PIN** - the PIN is locked on the 3G device's SIM card. **Unlock PUK fail** - Your attempt to unlock a WCDMA 3G device's PUK failed because you entered an incorrect PUK. **Unlock PIN fail** - Your attempt to unlock a WCDMA 3G device's PIN failed because you entered an incorrect PIN. **Unlock device fail** - Your attempt to unlock a CDMA2000 3G device failed because you entered an incorrect device code. **Device unlocked** - You entered the correct device code and unlocked a CDMA2000 3G device. **Get dev-info fail** - The ISG50 cannot get cellular device information. **Get dev-info ok** - The ISG50 succeeded in retrieving 3G device information. **Searching network** - The 3G device is searching for a network. **Get signal fail** - The 3G device cannot get a signal from a network. **Network found** - The 3G device found a network. **Apply config** - The ISG50 is applying your configuration to the 3G device. **Inactive** - The 3G interface is disabled. **Active** - The 3G interface is enabled. **Incorrect device** - The connected 3G device is not compatible with the ISG50. **Correct device** - The ISG50 detected a compatible 3G device. **Set band fail** - Applying your band selection was not successful. **Set band ok** - The ISG50 successfully applied your band selection. **Set profile fail** - Applying your ISP settings was not successful. **Set profile ok** - The ISG50 successfully applied your ISP settings. **PPP fail** - The ISG50 failed to create a PPP connection for the cellular interface. **Need auth-password** - You need to enter the password for the 3G card in the cellular edit screen. **Device ready** - The ISG50 successfully applied all of your configuration and you can use the 3G connection.
Service Provider	This displays the name of your network service provider. This shows **Limited Service** if the service provider has stopped service to the 3G SIM card. For example if the bill has not been paid or the account has expired.
Cellular System	This field displays what type of cellular network the 3G connection is using. The network type varies depending on the 3G card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM 3G card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA 3G card.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your ISG50 and the service provider's base station.

10.9.1 More Information

This screen displays more information on your 3G, such as the signal strength, IMEA/ESN and IMSI that helps identify your 3G device and SIM card. Click **Monitor > System Status > More Information** to display this screen.

Note: This screen is only available when the 3G device is attached to and activated on the ISG50.

Figure 151 Monitor > System Status > More Information



Extension Slot: USB 1
Service Provider: Chunghwa Telecom
Cellular System: WCDMA
Signal Strength: -91 dBm
Signal Quality: Fair
Device Manufacturer: Huawei
Device Model: E220/E270/E800/E180
Device Firmware: 076.11.07.106
Device IMEI / ESN: [redacted]
SIM Card IMSI: [redacted]

The following table describes the labels in this screen.

Table 43 Monitor > System Status > More Information

LABEL	DESCRIPTION
Extension Slot	This field displays where the entry's cellular card is located.
Service Provider	This displays the name of your network service provider. This shows **Limited Service** if the service provider has stopped service to the 3G SIM card. For example if the bill has not been paid or the account has expired.
Cellular System	This field displays what type of cellular network the 3G connection is using. The network type varies depending on the 3G card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM 3G card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA 3G card.
Signal Strength	This is the **Signal Quality** measured in dBm.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your ISG50 and the service provider's base station.
Device Manufacturer	This shows the name of the company that produced the 3G device.
Device Model	This field displays the model name of the cellular card.

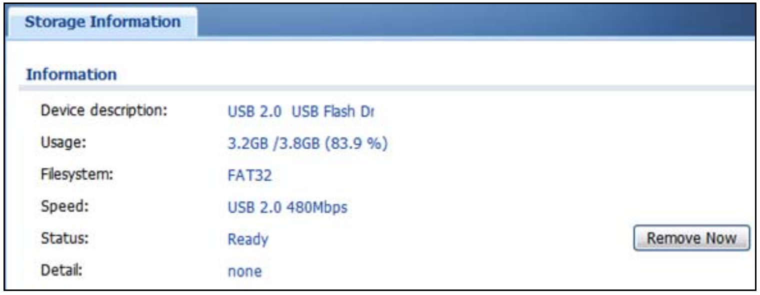
Table 43 Monitor > System Status > More Information

LABEL	DESCRIPTION
Device Firmware	This shows the software version of the 3G device.
Device IMEI/ESN	IMEI (International Mobile Equipment Identity) is a 15-digit code in decimal format that identifies the 3G device. ESN (Electronic Serial Number) is an 8-digit code in hexadecimal format that identifies the 3G device.
SIM Card IMSI	IMSI (International Mobile Subscriber Identity) is a 15-digit code that identifies the SIM card.

10.10 USB Storage Screen

This screen displays information about a connected USB storage device. Click **Monitor > System Status > USB Storage** to display this screen.

Figure 152 Monitor > System Status > USB Storage



Device description: USB 2.0 USB Flash Dr
Usage: 3.2GB /3.8GB (83.9 %)
Filesystem: FAT32
Speed: USB 2.0 480Mbps
Status: Ready
Detail: none

The following table describes the labels in this screen.

Table 44 Monitor > System Status > USB Storage

LABEL	DESCRIPTION
Device description	This is a basic description of the type of USB device.
Usage	This field displays how much of the USB storage device's capacity is currently being used out of its total capacity and what percentage that makes.
Filesystem	This field displays what file system the USB storage device is formatted with. This field displays **Unknown** if the file system of the USB storage device is not supported by the ISG50, such as NTFS.
Speed	This field displays the connection speed the USB storage device supports.

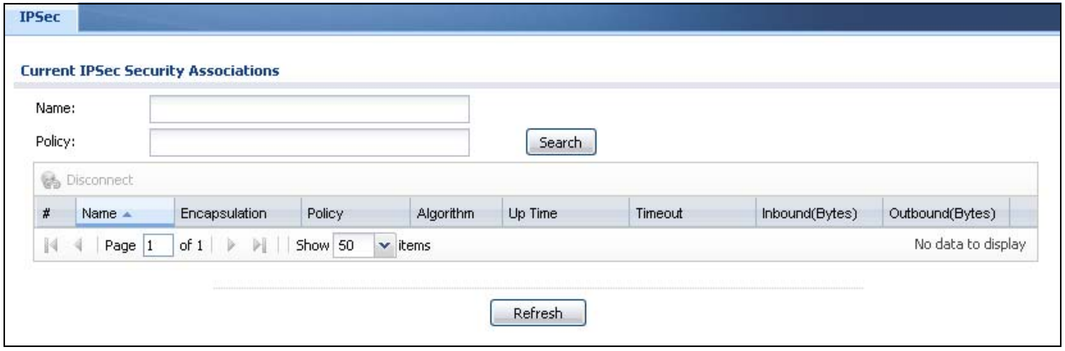
Table 44 Monitor > System Status > USB Storage (continued)

LABEL	DESCRIPTION
Status	**Ready** - you can have the ISG50 use the USB storage device. Click **Remove Now** to stop the ISG50 from using the USB storage device so you can remove it. **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the ISG50 cannot mount it. Click **Use It** to have the ISG50 mount a connected USB storage device. This button is grayed out if the file system is not supported (unknown) by the ISG50. **none** - no USB storage device is connected.
Detail	This field displays any other information the ISG50 retrieves from the USB storage device. **Deactivated** - the use of a USB storage device is disabled (turned off) on the ISG50. **OutofSpace** - the available disk space is less than the disk space full threshold (see Section 52.2 on page 666 for how to configure this threshold). **Mounting** - the ISG50 is mounting the USB storage device. **Removing** - the ISG50 is unmounting the USB storage device. **none** - the USB device is operating normally or not connected.

10.11 The IPSec Monitor Screen

You can use the **IPSec Monitor** screen to display and to manage active IPSec SAs. To access this screen, click **Monitor > VPN Monitor** > **IPSec**. The following screen appears. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 153 Monitor > VPN Monitor > IPSec


IPSec
Current IPSec Security Associations
Name:
Policy:
Search
Disconnect
#
Name
Encapsulation
Policy
Algorithm
Up Time
Timeout
Inbound(Bytes)
Outbound(Bytes)
Page 1 of 1
Show 50 items
No data to display
Refresh

Each field is described in the following table.

Table 45 Monitor > VPN Monitor > IPSec

LABEL	DESCRIPTION
Name	Enter the name of a IPSec SA here and click **Search** to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 10.11.1 on page 212 for more details.
Policy	Enter the IP address(es) or names of the local and remote policies for an IPSec SA and click **Search** to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 10.11.1 on page 212 for more details.
Search	Click this button to search for an IPSec SA that matches the information you specified above.
Disconnect	Select an IPSec SA and click this button to disconnect it.
Total Connection	This field displays the total number of associated IPSec SAs.
connection per page	Select how many entries you want to display on each page.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Policy	This field displays the content of the local and remote policies for this IPSec SA. The IP addresses, not the address objects, are displayed.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Up Time	This field displays how many seconds the IPSec SA has been active. This field displays **N/A** if the IPSec SA uses manual keys.
Timeout	This field displays how many seconds remain in the SA life time, before the ISG50 automatically disconnects the IPSec SA. This field displays **N/A** if the IPSec SA uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the ISG50 since the IPSec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the ISG50 to the remote IPSec router since the IPSec SA was established.
Refresh	Click **Refresh** to update the information in the display.

10.11.1 Regular Expressions in Searching IPSec SAs

A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.

Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use “*abc” (without the quotation marks) to specify any VPN connection or policy name that ends with “abc”. A VPN connection named “testabc” would match. There could be any number (of any type) of characters in front of the “abc” at the end and the VPN connection or policy name would still match. A VPN connection or policy name named “testacc” for example would not match.

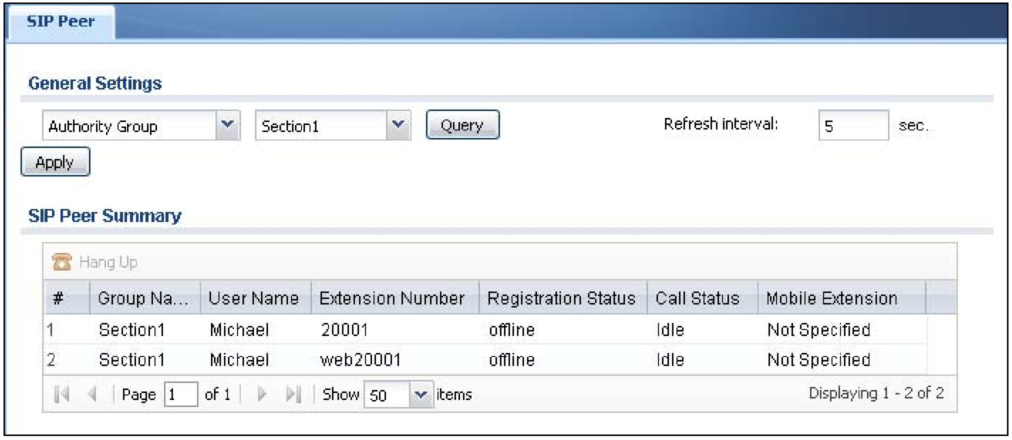
A * in the middle of a VPN connection or policy name has the ISG50 check the beginning and end and ignore the middle. For example, with “abc*123”, any VPN connection or policy name starting with “abc” and ending in “123” matches, no matter how many characters are in between.

The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

10.12 SIP Peer Screen

This screen displays information about the ISG50's SIP extensions. Click **Monitor > PBX > SIP Peer** to display this screen.

Figure 154 Monitor > PBX > SIP Peer



Authority Group

Section1

Refresh interval: 5 sec.

#	Group Na...	User Name	Extension Number	Registration Status	Call Status	Mobile Extension
1	Section1	Michael	20001	offline	Idle	Not Specified
2	Section1	Michael	web20001	offline	Idle	Not Specified

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

The following table describes the labels in this screen.

Table 46 Monitor > PBX > SIP Peer

LABEL	DESCRIPTION
General Settings	Use this section to specify your query criteria. You can select an attribute-value pair for your search. You can choose to query by: • Authority Group - select a specify authority group for which you want to view status details of SIP extensions. • Registration Status - select to view status details about SIP extension with which SIP devices have registered (online) or view status details about SIP extensions with which no SIP device is currently registered (offline). • Call Status - select whether you want to view status details about extensions that are currently busy or idle. Click **Query** to update the status detail table in the **SIP Peer Summary** section of the screen.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click **Apply** to update the screen immediately. If you do not want this screen to update periodically, enter **0**.
SIP Peer Summary	This section displays the status detail table.
#	This field is a sequential value, and it is not associated with a specific entry.
Group Name	This field displays the authority group name to which an extension belongs.
User Name	This field displays the user name associated with a SIP extension.
Extension Number	This field displays the SIP extension number. For each SIP extension there is also a web phone extension listed in the following format **web** + **extension number**. For example, extension **1001** also has a web phone extension **web1001** listed in this table. The web phone extensions allow you to see whether a web phone is being used for a specific SIP extension.

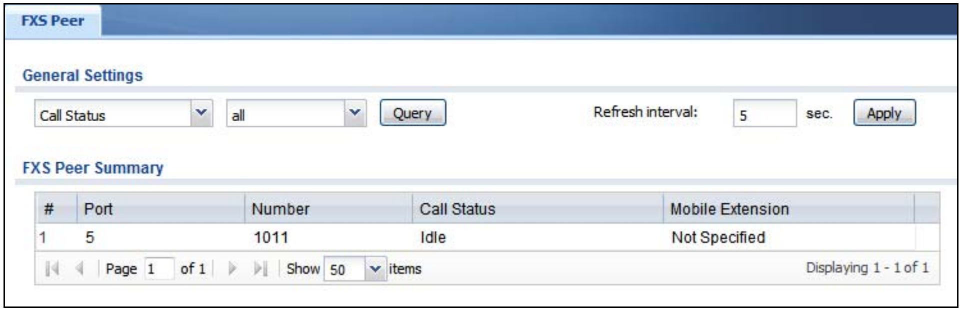
Table 46 Monitor > PBX > SIP Peer (continued)

LABEL	DESCRIPTION
Registration Status	This field displays **online**, if an IP phone is registered with the ISG50. It displays **offline** if no IP phone is registered with the ISG50 for a specific extension. For the web phone feature, it displays **online**, if a user has logged in the web phone feature, otherwise it displays **offline**.
Call Status	This field displays **busy** if a SIP extension is currently engaged, otherwise it displays **idle**.
Mobile Extension	This indicates whether the connection's mobile extension is activated or not, or if it is unspecified.
Hang Up	Click this to disconnect a connection.

10.13 FXS Peer Screen

This screen displays information about the ISG50's FXS extensions. Click **Monitor > PBX > FXS Peer** to display this screen.

Figure 155 Monitor > PBX > FXS Peer



Call Status: all

Refresh interval: 5 sec.

#	Port	Number	Call Status	Mobile Extension
1	5	1011	Idle	Not Specified

The following table describes the labels in this screen.

Table 47 Monitor > PBX > FXS Peer

LABEL	DESCRIPTION
General Settings	Use this section to specify your query criteria. You can select an attribute-value pair for your search. You can choose to query by: • Call Status - select whether you want to view status details about extensions that are currently busy or idle. Click **Query** to update the status detail table in the **FXS Peer Summary** section of the screen.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click **Apply** to update the screen immediately. If you do not want this screen to update periodically, enter **0**.
FXS Peer Summary	This section displays the status detail table.
#	This field is a sequential value, and it is not associated with a specific entry.
Port	This field displays the port number on the FXS port.
Number	This field displays the extension number associated with an FXS port or it displays **N/A**, if no FXS extension has been configured for an FXS port.

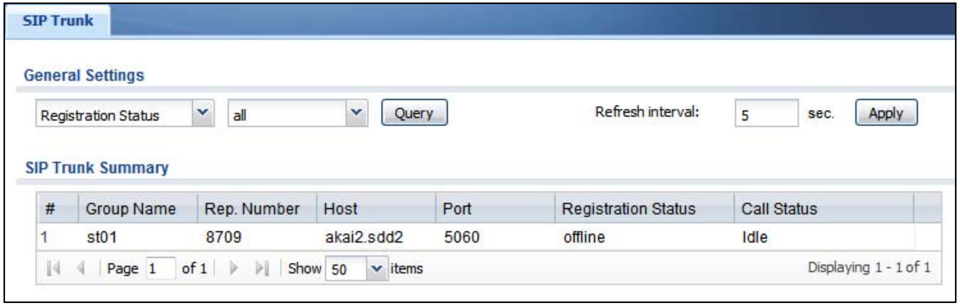
Table 47 Monitor > PBX > FXS Peer (continued)

LABEL	DESCRIPTION
Call Status	This field displays **busy** if an FXS extension is currently engaged, otherwise it displays **idle**.
Mobile Extension Status	This indicates whether the connection's mobile extension is activated or not, or if it is unspecified.

10.14 SIP Trunk Screen

This screen displays status information about external connections to other SIP servers. Click **Monitor > PBX > SIP Trunk** to display this screen.

Figure 156 Monitor > PBX > SIP Trunk



Registration Status: all

Refresh interval: 5 sec.

#	Group Name	Rep. Number	Host	Port	Registration Status	Call Status
1	st01	8709	akai2.sdd2	5060	offline	Idle

The following table describes the labels in this screen.

Table 48 Monitor > PBX > SIP Trunk

LABEL	DESCRIPTION
General Settings	Use this section to specify your query criteria. You can select an attribute-value pair for your search. You can choose to query by: • Registration Status - select to view status details about SIP trunks which have successfully registered with a SIP server (online), SIP trunks which are in the process of registering with a SIP server (Auth. Sent) or SIP trunks that have failed to register with a SIP server (offline). • Call Status - select whether you want to view status details about SIP trunks that are currently busy or idle. Click **Query** to update the status detail table in the **SIP Trunk Summary** section of the screen.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click **Apply** to update the screen immediately. If you do not want this screen to update periodically, enter **0**.
SIP Trunk Summary	This section displays the status detail table.
#	This field is a sequential value, and it is not associated with a specific entry.
Group Name	This field displays the outbound line group name of this SIP trunk.
Rep. Number	This field displays the caller number of an active call which its callee need use to call back.
Host	This field displays the IP address of the SIP server for the SIP server associated with this SIP trunk.
Port	This field displays the port number used for SIP communication with a SIP server.

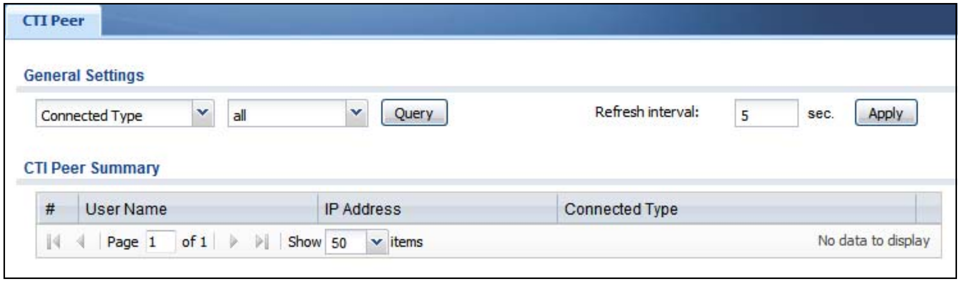
Table 48 Monitor > PBX > SIP Trunk (continued)

LABEL	DESCRIPTION
Registration Status	This field displays **online** if the ISG50 successfully registered with the SIP server for this SIP trunk, **offline** if the ISG50 failed to register with the SIP server for this SIP trunk or **Auth. Sent** if the ISG50 is in the process of registering with the SIP server associated with this SIP trunk.
Call Status	This field displays **busy** if a SIP line is currently engaged, otherwise it displays **idle**.

10.15 CTI Peer Screen

This screen displays status information about the ISG50's Computer Telephony Integration (CTI) connections. This screen displays which clients are registered through CTI. Click **Monitor > PBX > CTI Peer** to display this screen.

Figure 157 Monitor > PBX > CTI Peer



The following table describes the labels in this screen.

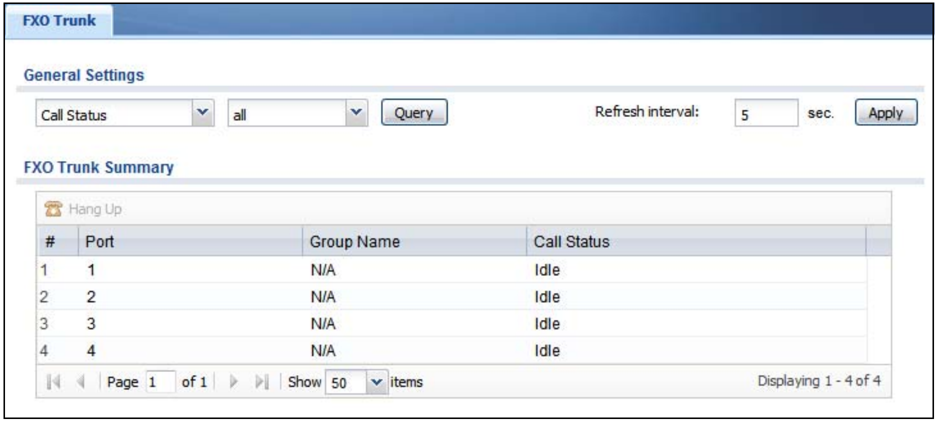
Table 49 Monitor > PBX > CTI Peer

LABEL	DESCRIPTION
General Settings	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: **Connected Type** - choose the type of CTI connection to filter for and display. Select all to display all CTI connections. Click **Query** to update the status detail table in the **CTI Peer Summary** section of the screen.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click **Apply** to update the screen immediately. If you do not want this screen to update periodically, enter **0**.
CTI Peer Summary	This section displays the status detail table.
#	This field is a sequential value, and it is not associated with a specific entry.
User Name	This displays the username that is making the connection.
IP Address	This displays the originating IP address of the connection.
Connected Type	This displays whether it is a TAPI server, TAPI client CTI connection.

10.16 FXO Trunk Screen

This screen displays status information about external connections via FXO interfaces. Click **Monitor > PBX > FXO Trunk** to display this screen.

Figure 158 Monitor > PBX > FXO Trunk



Call Status | all

Refresh interval: 5 sec.

#	Port	Group Name	Call Status
1	1	N/A	Idle
2	2	N/A	Idle
3	3	N/A	Idle
4	4	N/A	Idle

The following table describes the labels in this screen.

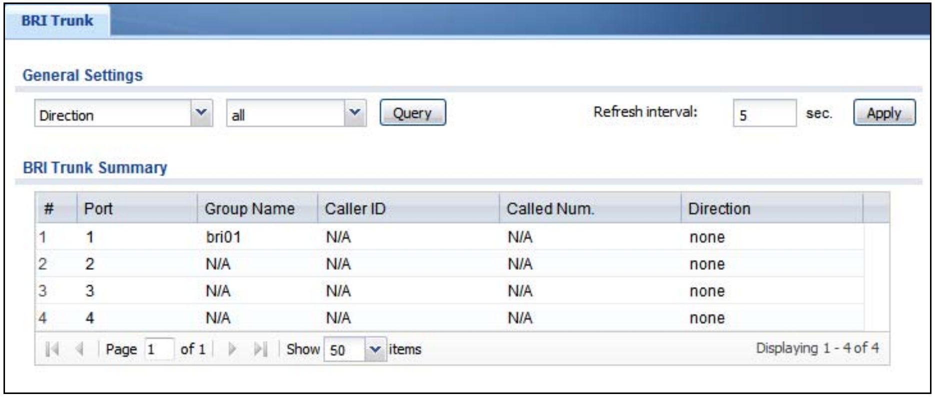
Table 50 Monitor > PBX > FXO Trunk

LABEL	DESCRIPTION
General Settings	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: • Call Status - select whether you want to view status details about FXO lines that are currently busy or idle. Click **Query** to update the status detail table in the **FXO Trunk Summary** section of the screen.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click **Apply** to update the screen immediately. If you do not want this screen to update periodically, enter **0**.
FXO Trunk Summary	This section displays the status detail table.
#	This field is a sequential value, and it is not associated with a specific entry.
Port	This field displays the port number on the FXO interface.
Group Name	This field displays the outbound line group name to which an FXO line is assigned.
Call Status	This field displays **Busy** if an FXO line is currently engaged. Otherwise, it displays **Idle**.
Hang Up	Click this to disconnect a connection.

10.17 BRI Trunk Screen

This screen displays status information about external connections via BRI interfaces. Click **Monitor > PBX > BRI Trunk** to display this screen.

Figure 159 Monitor > PBX > BRI Trunk



Direction: all

Refresh interval: 5 sec.

#	Port	Group Name	Caller ID	Called Num.	Direction
1	1	bri01	N/A	N/A	none
2	2	N/A	N/A	N/A	none
3	3	N/A	N/A	N/A	none
4	4	N/A	N/A	N/A	none

The following table describes the labels in this screen.

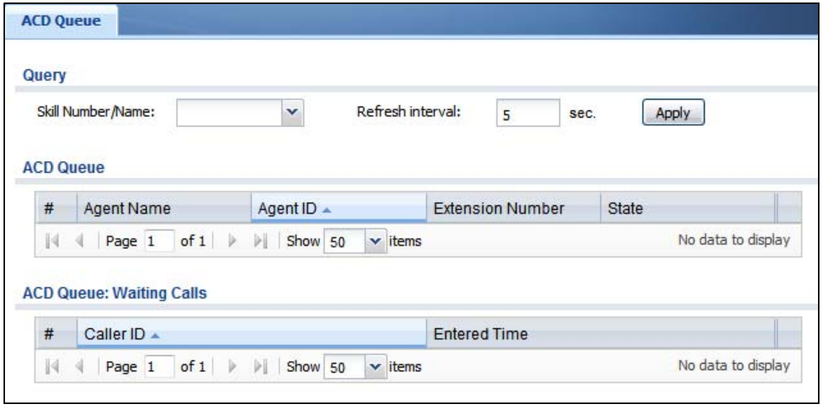
Table 51 Monitor > PBX > BRI Trunk

LABEL	DESCRIPTION
General Settings	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: • **Direction** - select which direction of calls you want to view status details about ISDN BRI lines. Select **In** for incoming calls, **Out** for outgoing calls or **all** for both incoming and outgoing calls. Alternatively, select **N/A** to display configured BRI trunk(s) without any calls over it. Click **Query** to update the status detail table in the **BRI Trunk Summary** section of the screen.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click **Apply** to update the screen immediately. If you do not want this screen to update periodically, enter **0**.
BRI Trunk Summary	This section displays the status detail table.
#	This field is a sequential value, and it is not associated with a specific entry.
Port	This field displays the port number of the ISDN BRI port.
Group Name	This field displays the outbound line group name to which an ISDN BRI line is assigned.
Caller ID	This field displays the caller identifier of a call or **N/A** for configured BRI trunk(s) without any calls over it.
Called Num.	This field displays the dialed number of a call or **N/A** for configured BRI trunk(s) without any calls over it.
Direction	This field displays **In** for an incoming call, **Out** for an outgoing call, **none** for configured BRI trunk(s) without any calls over it.

10.18 ACD Queue Screen

Use this screen to monitor phone call activity for Automatic Call Distribution (ACD) agents. Click **Monitor > PBX > ACD Queue** to display this screen.

Figure 160 Monitor > PBX > ACD Queue


ACD Queue
Query
Skill Number/Name:
Refresh interval:
5
sec.
Apply
ACD Queue
# | Agent Name | Agent ID | Extension Number | State
Page 1 of 1 | Show 50 items
No data to display
ACD Queue: Waiting Calls
# | Caller ID | Entered Time
Page 1 of 1 | Show 50 items
No data to display

The following table describes the labels in this screen.

Table 52 Monitor > PBX > ACD Queue

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: **Skill Number/Name** - Select the ACD skill number/name for which you want to view the statistics.
Refresh interval	Enter how often (seconds) you want the ISG50 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0.
ACD Queue	This table displays the current statistics for the queue on the selected **Skill Number/Name**.
#	This displays the number of entries in this table.
Agent Name	This displays the name of an agent associated with the selected skill/number.
Agent ID	This displays the ID numbers of an agent associated with the selected skill/number.
Extension Number	This displays the extension of an agent associated with the selected skill/number.
State	This displays the current state of an agent associated with the selected skill/number. **Idle** - This indicates the agent associated with the selected skill/number is logged in and idle. **Busy (skill_XXXXX)** - This indicates the agent associate with the selected skill/number is logged and busy. The skill that appears in parentheses indicates the skill with which he is currently occupied, if he belongs to multiple skills. **Pause** - This indicates the agent associated with the selected skill/number is logged in and his account is currently paused (not receiving or making calls). **Logoff** - This indicates the agent associated with the selected skill/number is not logged in.
Priority	This indicates the priority rating of the agent associated with the selected skill/number.
ACD Queue: Waiting Calls	This table displays a list all calls currently waiting in the queue for the selected skill/number.

Table 52 Monitor > PBX > ACD Queue (continued)

LABEL	DESCRIPTION
Caller ID	This indicates the caller ID of the call.
Entered Time	This indicates the time the caller entered the queue.
Waiting Time	This indicates how long the caller has been waiting in the queue.

10.19 Log Screen

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, firewall or user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

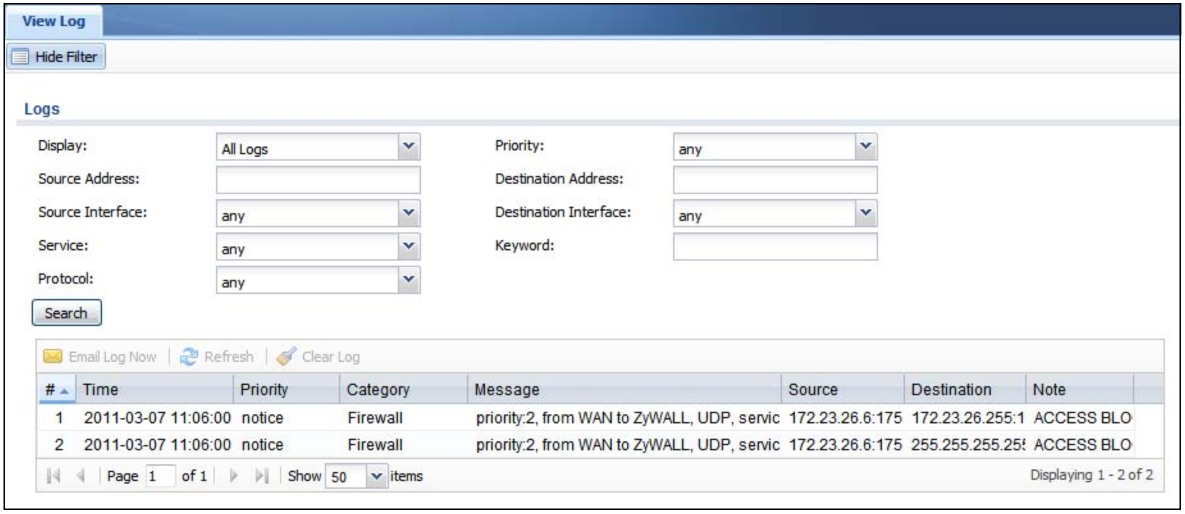
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

- For individual log descriptions, see Appendix A on page 775.
- For the maximum number of log messages in the ISG50, see .

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 161 Monitor > Log



Display: All Logs
Priority: any
Source Address:
Destination Address:
Source Interface: any
Destination Interface: any
Service: any
Keyword:
Protocol: any

#	Time	Priority	Category	Message	Source	Destination	Note
1	2011-03-07 11:06:00	notice	Firewall	priority:2, from WAN to ZyWALL, UDP, servic	172.23.26.6:175	172.23.26.255:1	ACCESS BLO
2	2011-03-07 11:06:00	notice	Firewall	priority:2, from WAN to ZyWALL, UDP, servic	172.23.26.6:175	255.255.255.25!	ACCESS BLO

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

The following table describes the labels in this screen.

Table 53 Monitor > Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Service**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Service	This displays when you show the filter. Select the service whose log messages you would like to see. The Web Configurator uses the protocol and destination port number(s) of the service to select which log messages you see.
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Email Log Now	Click this button to send log message(s) to the **Active** e-mail address(es) specified in the **Send Log To** field on the **Log Settings** page (see Section 53.3.2 on page 710).
Refresh	Click this button to update the information in the screen.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on (see **Log Consolidation** in Table 285 on page 711) and multiple entries were aggregated to generate into this one.

Table 53 Monitor > Log (continued)

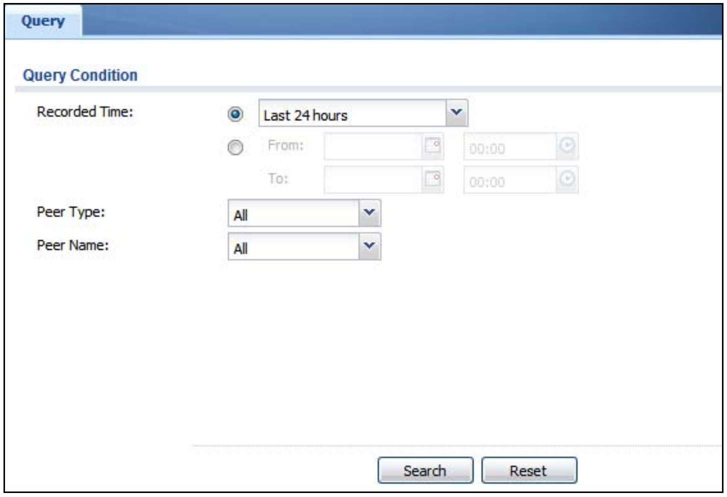
LABEL	DESCRIPTION
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

The Web Configurator saves the filter settings if you leave the **View Log** screen and return to it later.

10.20 Querying Call Recordings

Use this screen to search for call recordings on the ISG50. Click **Monitor > Log > Call Recording** to open the screen as following.

Figure 162 Call Recording Query



Recorded Time: ● Last 24 hours
○ From: 00:00
To: 00:00
Peer Type: All
Peer Name: All

The following table describes the labels in this screen.

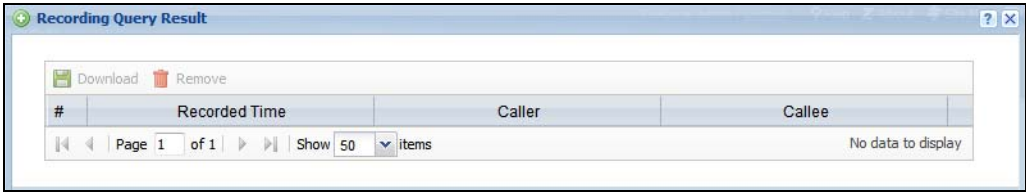
Table 54 Call Recording Query

LABEL	DESCRIPTION
Recorded Time	Select the first option to look for call recordings from the past day, week, or month. Select the line to not specify a time period. Select the second option to be able to specify an exact time period for which to find call recordings. Enter the starting and ending year, month, day, hour, minute, and seconds look for call recordings from the past day, week, or month. Click the button to open a calendar for entering the date.
Peer Type	Specify whether you want to find call recordings for trunks, extensions, or both.
Peer Name	Select the trunk or extension for which you want to find call recordings.
Search	Click this to display a list of call recordings that match your specified criteria.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.20.1 Call Recordings File List

This screen lists the call recordings that matched your specified criteria. Use this screen to listen to or delete individual call recordings. Click **Monitor > Log > Call Recording** and perform a query to open the screen as following.

Figure 163 Call Recordings File List


Recording Query Result
Download
Remove
#
Recorded Time
Caller
Callee
Page 1 of 1
Show 50 items
No data to display

The following table describes the labels in this screen.

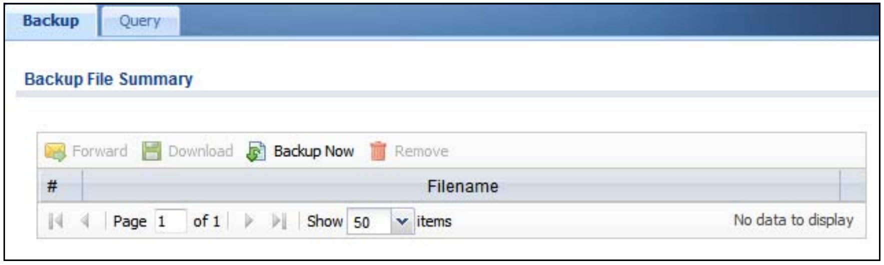
Table 55 Call Recordings File List

LABEL	DESCRIPTION
Download	Select an entry and click **Download** to save the call recording to your computer.
Remove	Select an entry or entries and click **Remove** to delete them from the ISG50.
#	This is the number of the entry in the list.
Recorded Time	This is the time that the call recording started. Click an entry to play the call recording.
Caller	This is the number that initiated the call. This cell is highlighted if the number is for a peer in the recording list.
Callee	This is the number that received the call. This cell is highlighted if the number is for a peer in the recording list.

10.21 CDR Backup Screen

Use this screen to backup CDR files, delete existing backups of CDR files and mail CDR files to an administrator email address. Click **Monitor > Log > CDR** to open this screen.

Figure 164 Monitor > Log > CDR


Backup
Query
Backup File Summary
Forward
Download
Backup Now
Remove
#
Filename
Page 1 of 1
Show 50 items
No data to display

Each field is described in the following table.

Table 56 Monitor > Log > CDR

LABEL	DESCRIPTION
Forward	Select the files you want to forward to the administrator email address and click the **Forward** button.
Download	Select an entry and click **Download** to save it to your computer.

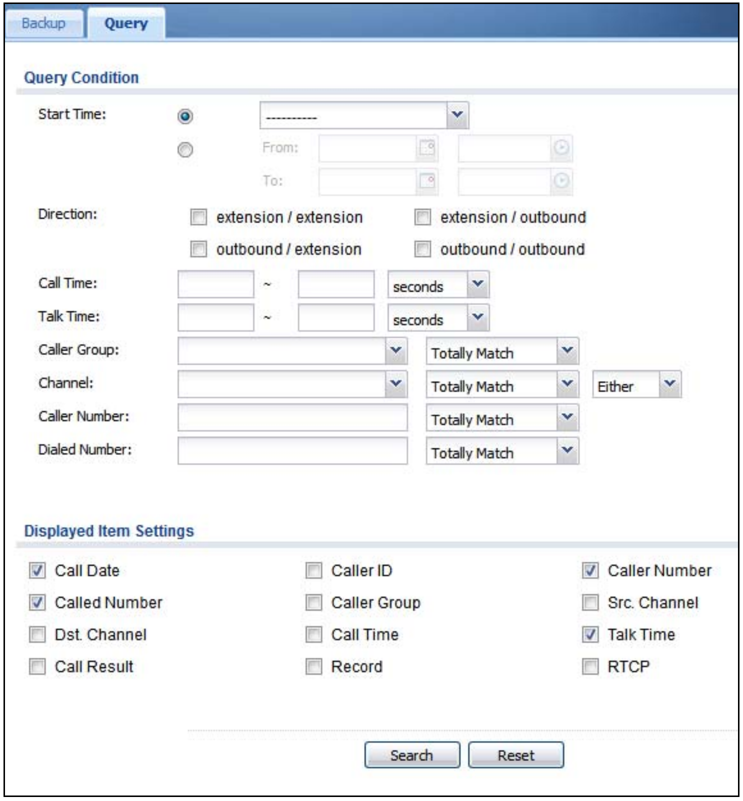
Table 56 Monitor > Log > CDR (continued)

LABEL	DESCRIPTION
Backup Now	Click the **Backup Now** button to save a CDR backup file on the ISG50.
Remove	If you no longer want to store a CDR file on the ISG50 then select the files you want to delete from the ISG50 and click the **Remove** button.
#	This is the number of the entry in the list.
Filename	This column displays the names of the backup CDR files currently stored on the ISG50. Use the check box on the left to specify which files you want to forward or delete. The filename of the CDR takes the “cdr.YYYYMMDDHHMMSS.sgi.tgz” or “cdr.YYYYMMDDHHMMSS.csv.tgz” format. Where: • **cdr** - indicates this is a Call Detail Record file. • **YYYYMMDD** - is the year, month, and day indicating when the backup file was created. • **HHMMSS** - is the time of the day indicating when the backup file was created in hour, minute, second format. • **tgz** - indicates that this is a compressed. That can be decompressed using a compression utility such as WinRAR. The resulting decompressed files are MySQL database files that can be managed via a MySQL DBMS (Database Management System). See CDR Database Management via PostgreSQL on page 721. Note: The ISG50 can store only three CDR backup files at a time. If you create a new backup file when you already have three files created, then the oldest backup file is deleted from the system.

10.22 CDR Query Screen

Use this screen to search for call records on the ISG50. Click **Monitor > Log > CDR > Query** to view the screen as shown next. See Viewing Aged Files on page 720 for details about extension ".tgz" files.

Figure 165 Monitor > Log > CDR > Query



Query Condition

Start Time: ● ---------- ○ From: To:

Direction:
☐ extension / extension
☐ extension / outbound
☐ outbound / extension
☐ outbound / outbound

Call Time: ~ seconds

Talk Time: ~ seconds

Caller Group: Totally Match

Channel: Totally Match Either

Caller Number: Totally Match

Dialed Number: Totally Match

Displayed Item Settings

☑ Call Date
☑ Called Number
☐ Dst. Channel
☐ Call Result
☐ Caller ID
☐ Caller Group
☐ Call Time
☐ Record
☑ Caller Number
☐ Src. Channel
☑ Talk Time
☐ RTCP

Each field is described in the following table.

Table 57 Monitor > Log > CDR > Query

LABEL	DESCRIPTION
Query Condition	Use this section to specify your query details.
Start Time	Specify the time period for your query. Choose a specific time period from the drop down list box or fill in the **From** and **To** fields with the time range you want to search the call detail record. You can use the pop-up calendar to fill in the date fields for the **To** and **From** fields by clicking the calendar buttons and selecting the date.
Direction	Specify the types of calls you want to view based on the source and destination of the calls. You can choose one or more of the available source - destination combinations: • **extension / extension** - to view internal calls; those made from one extension to another extension on the ISG50. • **extension / outbound** - to view calls from within your organization made to the outside world via one of the outbound lines. • **outbound / extension** - to view calls from the outside world to extensions configured on the ISG50. • **outbound / outbound** - to view calls that come in from an outbound line and are routed back to the outside world via another outbound line.

Table 57 Monitor > Log > CDR > Query (continued)

LABEL	DESCRIPTION
Call Time	Call time is the time from when a caller finishes dialing a number until one of the parties hangs up. Enter the range of seconds, minutes or hours to specify the length of calls that you want to search for. If you leave this field blank, then the length of the call will not be considered as a search criterion, in other words calls of all length duration are displayed unless limited by other search criteria.
Talk Time	Talk time is the time from when a callee picks up an incoming call until one of the parties hangs up. Enter the range of seconds, minutes or hours to specify the length of calls that you want to search for. If you leave this field blank, then the length of the call will not be considered as a search criterion, in other words calls of all length duration are displayed unless limited by other search criteria.
Caller Group	Type the name of the authority group or outbound line group for which you want to search the call detail record. Use the drop down list box to choose **Totally Match**, if you want to display only call records that exactly match the criteria you type or select **Partially Match**, if you want to enter only a part of the group name that you want to search for. Alternatively, use the drop-down list box to select the outbound line group or authority group configured on the ISG50 that you want to use as your search criterion.
Channel	Type the name of the type of channel for which you want to search the call detail record. The channels can be either FXS extensions, FXO outbound channels, or SIP based connections. Use the drop down list box to choose **Totally Match**, if you want to display only call records that exactly match the criteria you type in or select **Partially Match** if you want to enter only a part of the group name that you want to search for. Alternatively, use the drop-down list box to select the channel configured on the ISG50 that you want to use as your search criterion. Next use the drop down list box to select whether you want to search calls originating from this channel (**SRC.**), terminating via this channel (**Dest.**) or both (**Both**).
Caller Number	Type the telephone number of the caller for which you want to search the call detail record. Use the drop down list box to choose **Totally Match**, if you want to display only call records that exactly match the criteria you type in or select **Partially Match,** if you want to enter only a part of the telephone number to search for.
Dialed Number	Type the dialed telephone number of the callee for which you want to search the call detail record. Use the drop down list box to choose **Totally Match**, if you want to display only call records that exactly match the criteria you type in or select **Partially Match**, if you want to enter only a part of the telephone number to search for.
Displayed Item Setting	Use this section to specify which details you want to display in the CDR report for each telephone call record displayed. You can choose to display the following details: • **Call Date** - The date and time the call took place (start time). • **Caller ID** - The username associated with the extension that partook in the call. • **Caller Number** - The telephone number from which the call originated. • **Called Number** - The telephone number of a callee. • **Caller Group** - The authority group of the extension that partook in the call or the outbound line group used to make the call. • **Src. Channel** - the interface type (FXS, FXO or SIP) and name from which this call originated. • **Dst. Channel** - The type of outbound line group, if the callee is outside your organization or the extension type (SIP or FXS) if the callee is within your organization. • **Call Time** - The total duration of the call from the time the ringing started until one of the parties hung up. • **Talk Time** - The total time of the call from the time the callee picked up the call until one of the parties hung up. • **Call Result** - “Answered” if the call was completed successfully, “Not Answered” if the call was not answered. • **Record** - Whether or not the call was recorded on the ISG50. • **RTCP** - RTCP information for voice quality troubleshooting.

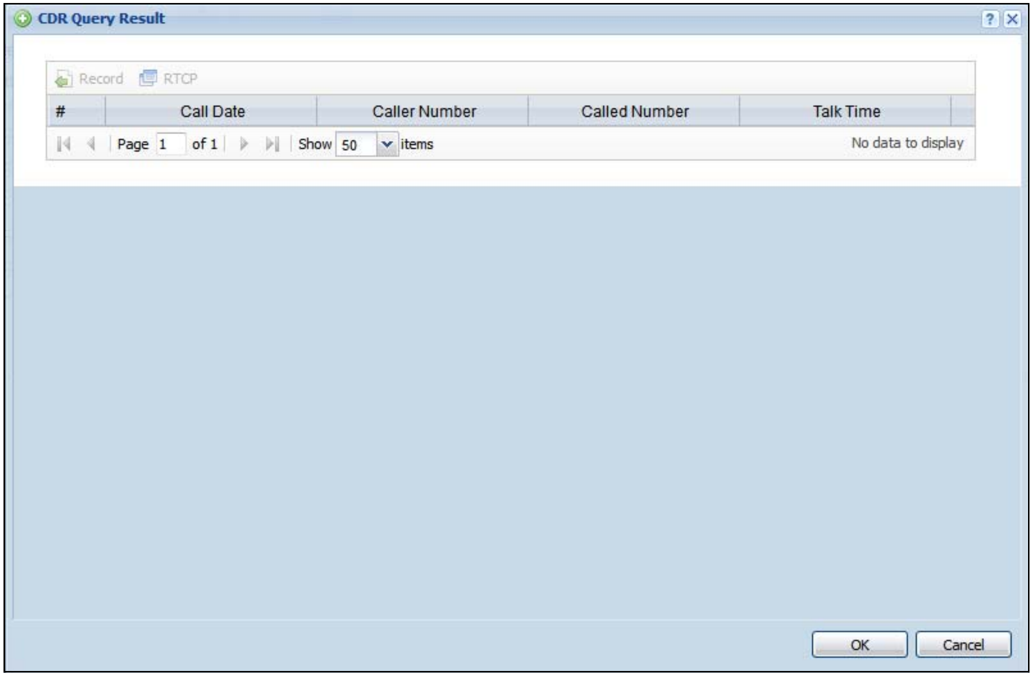
Table 57 Monitor > Log > CDR > Query (continued)

LABEL	DESCRIPTION
Search	Click the **Search** button to display your query results in a report window. Your Internet browser opens up a new window with the query results.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.23 CDR Query Result Screen

This screen displays the results of your search for call records on the ISG50. Click **Monitor > Log > CDR > Query** and perform a search to view the screen as shown next. The details listed depends on which details you selected in the query screen. See Section 10.22 on page 225 for more information.

Figure 166 Monitor > Log > CDR > Query > Result



Each field is described in the following table.

Table 58 Monitor > Log > CDR > Query > Result

LABEL	DESCRIPTION
Record	Select a record entry and click **Record** to save the entry to your computer.
RTCP	Select a record entry and click **RTCP** to view RTCP information for voice quality troubleshooting.
#	This field is a sequential value and is not associated with any entry.
	The format of your report depends on the details you selected in the query screen. See Section 10.22 on page 225 for details.
Search	Click the **Search** button to display your query results in a report window. Your Internet browser opens up a new window with the query results.
Reset	Click **Reset** to return the screen to its last-saved settings.

11

Registration

11.1 Overview

Use the **Configuration > Licensing > Registration** screens to register your ISG50 and manage its service subscriptions.

11.1.1 What You Can Do in this Chapter

- Use the **Registration** screen (see Section 11.2 on page 230) to register your ISG50 with myZyXEL.com and activate a service.
- Use the **Service** screen (see Section 11.3 on page 231) to display the status of your service registrations and upgrade licenses.

11.1.2 What you Need to Know

This section introduces the topics covered in this chapter.

myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your ISG50 and manage subscription services available for the ISG50. To use a subscription service, you have to register the ISG50 and activate the corresponding service at myZyXEL.com (through the ISG50).

Note: You need to create a myZyXEL.com account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ISG50 and activate a service using the **Registration** screen. Alternatively, go to http://www.myZyXEL.com with the ISG50's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a ISG50, you need to access myZyXEL.com via that ISG50.

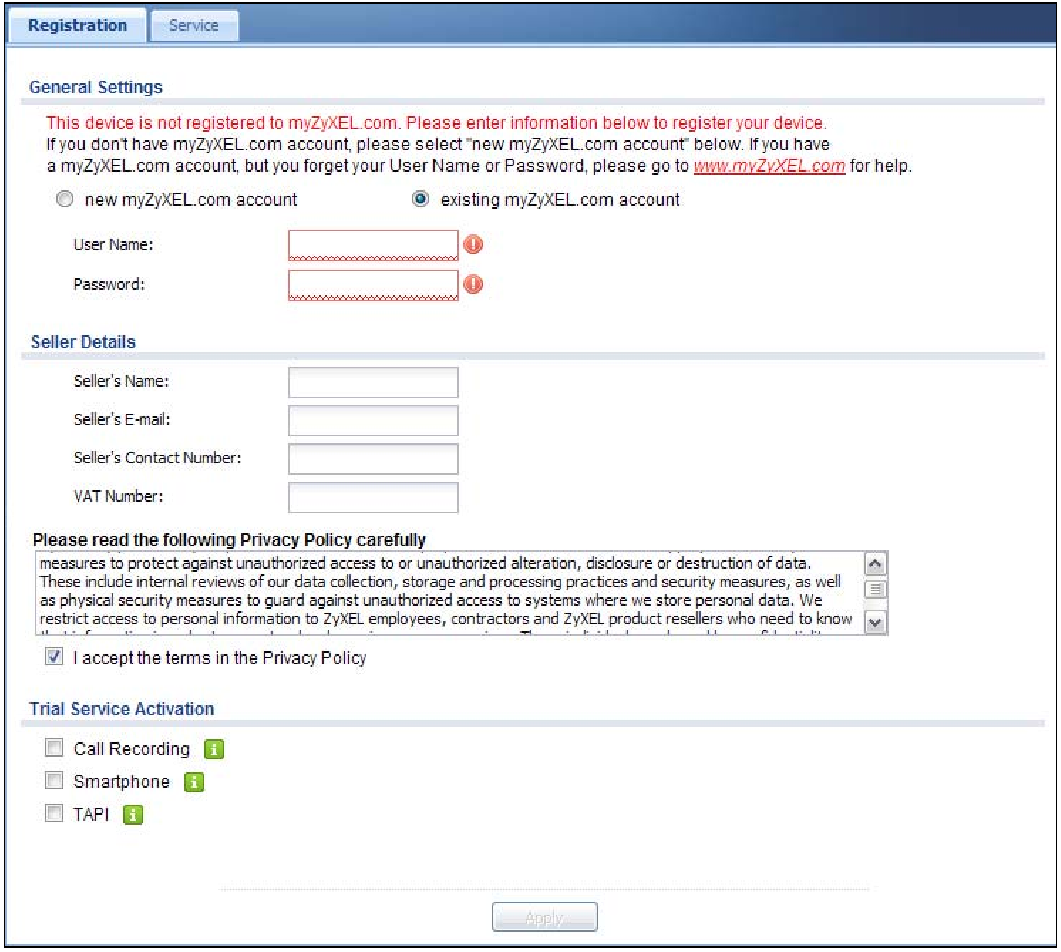
Subscription Services Available on the ISG50

Purchase and enter a license key to use subscription services such as call recording, additional extension numbers, and smartphone application support. You can try a free trial of the call recording and smartphone application support services. See the respective User's Guide chapters for more information about these features.

11.2 The Registration Screen

Use this screen to register your ISG50 with myZyXEL.com and activate a service, such as additional SIP extension numbers. Click **Configuration > Licensing > Registration** in the navigation panel to open the screen as shown next.

Figure 167 Configuration > Licensing > Registration



This device is not registered to myZyXEL.com. Please enter information below to register your device.
If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have a myZyXEL.com account, but you forget your User Name or Password, please go to www.myZyXEL.com for help.

○ new myZyXEL.com account ● existing myZyXEL.com account

Please read the following Privacy Policy carefully

measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data. We restrict access to personal information to ZyXEL employees, contractors and ZyXEL product resellers who need to know

☑ I accept the terms in the Privacy Policy

☐ Call Recording
☐ Smartphone
☐ TAPI

The following table describes the labels in this screen.

Table 59 Configuration > Licensing > Registration

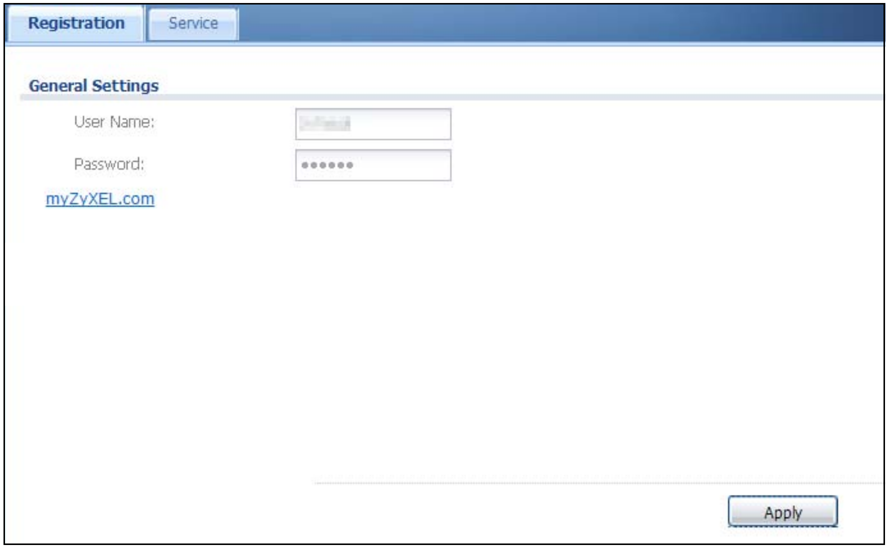
LABEL	DESCRIPTION
General Settings	If you select **existing myZyXEL.com account**, only the **User Name** and **Password** fields are available.
new myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ISG50.
existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ISG50.
User Name	Enter a user name for your myZyXEL.com account. The name should be from 6 to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.

Table 59 Configuration > Licensing > Registration (continued)

LABEL	DESCRIPTION
Password	Enter a password of between 6 and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country	Select your country from the drop-down box list.
Seller Details	Use this section to enter your seller information.
Seller's Name	Enter your seller's name.
Seller's E-mail	Enter your seller's e-mail address.
Seller's Contact Number	Enter your seller's phone number.
VAT Number	Enter your seller's Value-Added Tax number, if you bought your ISG50 from Europe.
I accept the terms in the Privacy Policy	If you accept the privacy policy statement shown above this field, select this check box.
Trial Service Activation	Select the check box to activate a trial service subscription. The trial period starts the day you activate the trial. After the trial expires, you can buy an iCard and enter the license key in the **Registration Service** screen to extend the service.
Apply	Click **Apply** to save your changes back to the ISG50.

Note: If the ISG50 is registered already, this screen is read-only and indicates whether trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Service** screen to update your service subscription status.

Figure 168 Configuration > Licensing > Registration: Registered Device



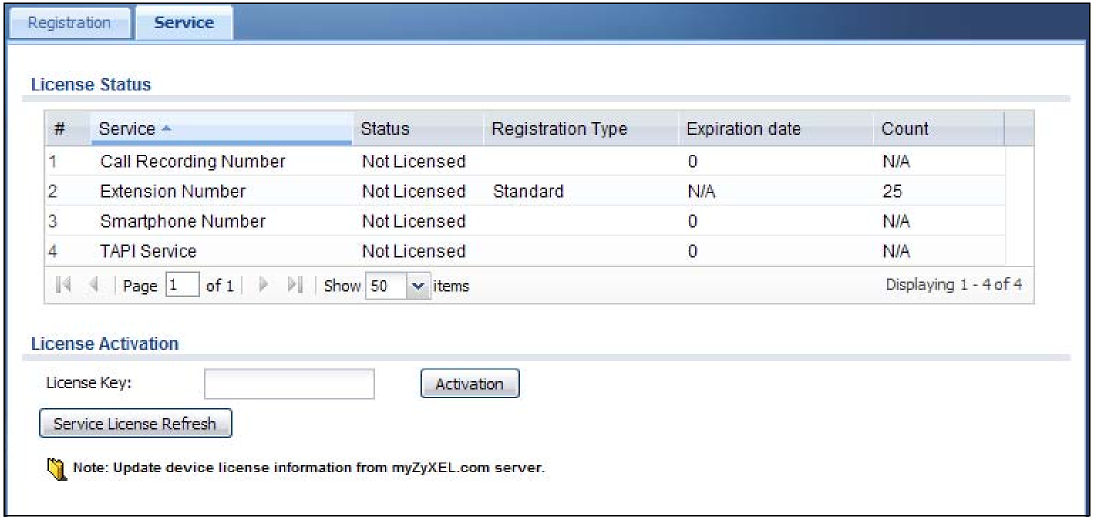
User Name:

Password: ••••••

11.3 The Service Screen

Use this screen to display the status of your service registrations and upgrade licenses. To activate or extend a standard service subscription, purchase an iCard and enter the iCard's PIN number (license key) in this screen. Click **Configuration > Licensing > Registration** > **Service** to open the screen as shown next.

Figure 169 Configuration > Licensing > Registration > Service



License Status

#	Service	Status	Registration Type	Expiration date	Count
1	Call Recording Number	Not Licensed		0	N/A
2	Extension Number	Not Licensed	Standard	N/A	25
3	Smartphone Number	Not Licensed		0	N/A
4	TAPI Service	Not Licensed		0	N/A

Page 1 of 1 Show 50 items Displaying 1 - 4 of 4

License Activation

License Key:

Note: Update device license information from myZyXEL.com server.

The following table describes the labels in this screen.

Table 60 Configuration > Licensing > Registration > Service

LABEL	DESCRIPTION
License Status	
#	This is the entry's position in the list.
Service	This lists the services that available on the ISG50.
Status	This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**).
Registration Type	This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). This field is blank when a service is not activated.
Expiration date	This field displays the date your service expires.
Count	This field displays how many instances of a service you can use with your current license. This field does not apply to the other services.
License Activation	
License Key	Enter your iCard's PIN number and click **Activation** to activate or extend a standard service subscription. If a standard service subscription runs out, you need to buy a new iCard (specific to your ISG50) and enter the new PIN number to extend the service.
Service License Refresh	Click this button to renew service license information (such as the registration status and expiration day).

12

Interfaces

12.1 Interface Overview

Use the **Interface** screens to configure the ISG50's interfaces. You can also create interfaces on top of other interfaces.

- **Ports** are the physical ports to which you connect cables.
- **Interfaces** are used within the system operationally. You use them in configuring various features. An interface also describes a network that is directly connected to the ISG50. For example, You connect the LAN1 network to the LAN1 interface.
- **Zones** are groups of interfaces used to ease security policy configuration.

12.1.1 What You Can Do in this Chapter

- Use the **Port Role** screens (Section 12.2 on page 236) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the **Ethernet** screens (Section 12.3 on page 237) to configure the Ethernet interfaces. Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- Use the **PPP** screens (Section 12.4 on page 246) for PPPoE or PPTP Internet connections.
- Use the **Cellular** screens (Section 12.5 on page 251) to configure settings for interfaces for Internet connections through an installed 3G card.
- Use the **VLAN** screens (Section 12.6 on page 259) to divide the physical network into multiple logical networks. VLAN interfaces receive and send tagged frames. The ISG50 automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Use the **Bridge** screens (Section 12.7 on page 267) to combine two or more network segments into a single network.
- Use the **Virtual Interface** screen (Section 12.7.3 on page 275) to create virtual interfaces on top of Ethernet interfaces to tell the ISG50 where to route packets. You can create virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- Use the **Trunk** screens (Chapter 13 on page 281) to configure load balancing.

12.1.2 What You Need to Know

Interface Characteristics

Interfaces generally have the following characteristics (although not all characteristics apply to each type of interface).

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.

- Many interfaces can share the same physical port.
- An interface belongs to at most one zone.
- Many interfaces can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Types of Interfaces

You can create several types of interfaces in the ISG50.

- Setting interfaces to the same port role forms a port group. Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ISG50 automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ISG50. You can also assign an IP address and subnet mask to the bridge.
- **PPP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Cellular interfaces** are for 3G WAN connections via a connected 3G device.
- **Virtual interfaces** provide additional routing information in the ISG50. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- **Trunk interfaces** manage load balancing between interfaces.

Port groups and trunks have a lot of characteristics that are specific to each type of interface. See Section 12.2 on page 236 and Chapter 13 on page 281 for details. The other types of interfaces--Ethernet, PPP, cellular, VLAN, bridge, and virtual--have a lot of similar characteristics. These characteristics are listed in the following table and discussed in more detail below.

Table 61 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
Name*	wan1, wan2	lan1, lan2, dmz	ppp*x*	cellularx	vlan*x*	br*x*	**
Configurable Zone	No	No	No	No	Yes	Yes	No
IP Address Assignment							
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters							
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	Yes	No
DHCP							
DHCP server	No	Yes	No	No	Yes	Yes	No
DHCP relay	No	Yes	No	No	Yes	Yes	No
Connectivity Check	Yes	No	Yes	No	Yes	Yes	No

- * The format of interface names other than the Ethernet and ppp interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, lan1, lan2, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

Relationships Between Interfaces

In the ISG50, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports or port groups. The relationships between interfaces are explained in the following table.

Table 62 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
port group	physical port
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPP interface	WAN1, WAN2
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	 Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPP interface

* - You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

Finding Out More

- See Section 6.3 on page 92 details on the differences between physical ports, interfaces, and zones in the ISG50.
- See Section 6.6.3 on page 98 for related information about the **Interface** screens.
- See Section 12.8 on page 276 for background information on interfaces.
- See Section 7.1 on page 107 for an example of configuring Ethernet interfaces, port role, and zones.
- See Section 7.2 on page 109 for an example of configuring a cellular (3G) interface.
- See Chapter 13 on page 281 to configure load balancing using trunks.

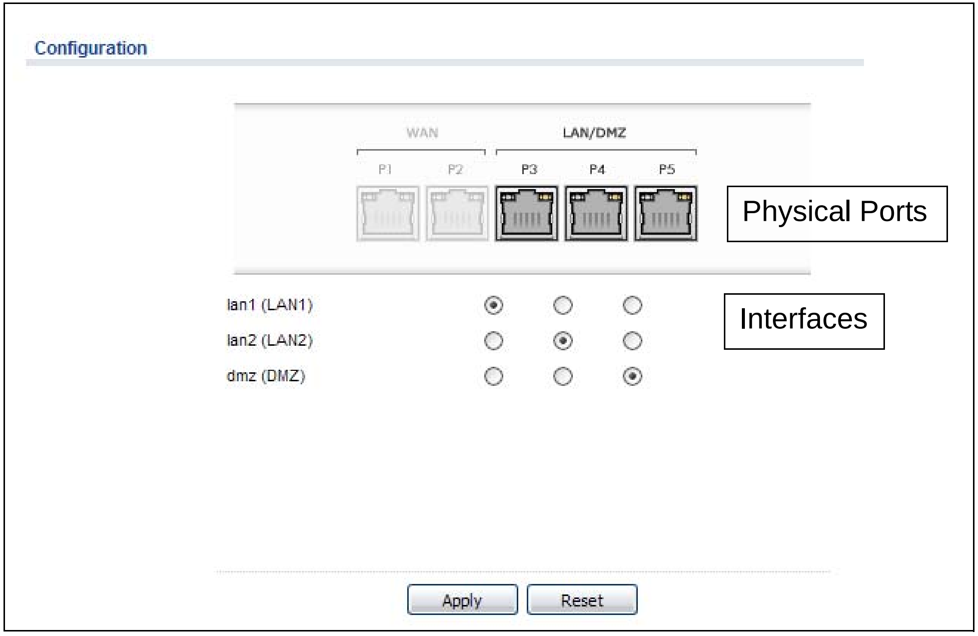
12.2 Port Role

To access this screen, click **Configuration > Network** > **Interface** > **Port Role**. Use the **Port Role** screen to set the ISG50’s flexible ports as part of the **lan1**, **lan2** or **dmz** interfaces. This creates a hardware connection between the physical ports at the layer-2 (data link, MAC address) level. This provides wire-speed throughput but no security.

Note the following if you are configuring from a computer connected to a **lan1**, **lan2** or **dmz** port and change the port's role:

1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ISG50's **lan1**, **lan2** or **dmz** IP address.
2. Use the appropriate **lan1**, **lan2** or **dmz** IP address to access the ISG50.

Figure 170 Configuration > Network > Interface > Port Role



lan1 (LAN1)	●	○	○
lan2 (LAN2)	○	●	○
dmz (DMZ)	○	○	●

Each section in this screen is described below.

Table 63 Configuration > Network > Interface > Port Role

LABEL	DESCRIPTION
P1 ~P5	These are physical Ethernet ports.
lan1 (LAN1) lan2 (LAN2) dmz (DMZ)	These are Ethernet interfaces and the zone to which each belongs. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port’s **lan1 (LAN1)** radio button to use the port as part of the lan1 interface. The port will use the ISG50’s lan1 IP address and MAC address. When you assign more than one physical port to a network, you create a **port group**. Port groups have the following characteristics: • There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security. • It can increase the bandwidth between the port group and other interfaces. • The port group uses a single MAC address.

Table 63 Configuration > Network > Interface > Port Role (continued)

LABEL	DESCRIPTION
Apply	Click this button to save your changes and apply them to the ISG50.
Reset	Click this button to change the port groups to their current configuration (last-saved values).

12.3 Ethernet Summary Screen

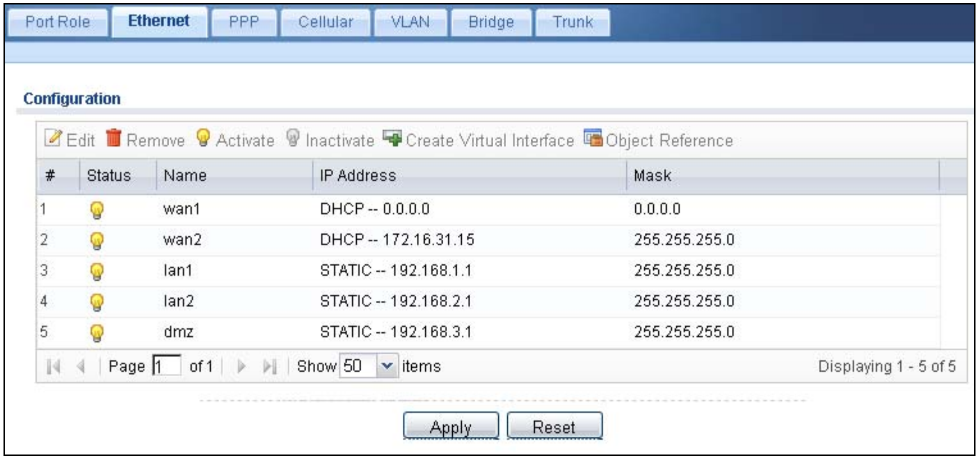
This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. To access this screen, click **Configuration > Network** > **Interface > Ethernet**.

Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of them. If an Ethernet interface does not have any physical ports assigned to it (see Section 12.2 on page 236), the Ethernet interface is effectively removed from the ISG50, but you can still configure it.

Ethernet interfaces are similar to other types of interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict the amount of bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

Use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management. The ISG50 supports two routing protocols, RIP and OSPF. See Chapter 15 on page 302 for background information about these routing protocols.

Figure 171 Configuration > Network > Interface > Ethernet



#	Status	Name	IP Address	Mask
1	💡	wan1	DHCP -- 0.0.0.0	0.0.0.0
2	💡	wan2	DHCP -- 172.16.31.15	255.255.255.0
3	💡	lan1	STATIC -- 192.168.1.1	255.255.255.0
4	💡	lan2	STATIC -- 192.168.2.1	255.255.255.0
5	💡	dmz	STATIC -- 192.168.3.1	255.255.255.0

Each field is described in the following table.

Table 64 Configuration > Network > Interface > Ethernet

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a virtual interface, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an interface, select it and click **Activate**.
Inactivate	To turn off an interface, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual Ethernet interface, select an Ethernet interface and click **Create Virtual Interface**.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.3.1 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, connectivity check, and MAC address settings. To access this screen, click an **Edit** icon in the **Ethernet Summary** screen. (See Section 12.3 on page 237.)

The WAN interface's **Edit > Configuration** screen is shown here as an example.

Note: If you create IP address objects based on an interface's IP address, subnet, or gateway, the ISG50 automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change LAN1's IP address, the ISG50 automatically updates the corresponding interface-based, LAN1 subnet address object.

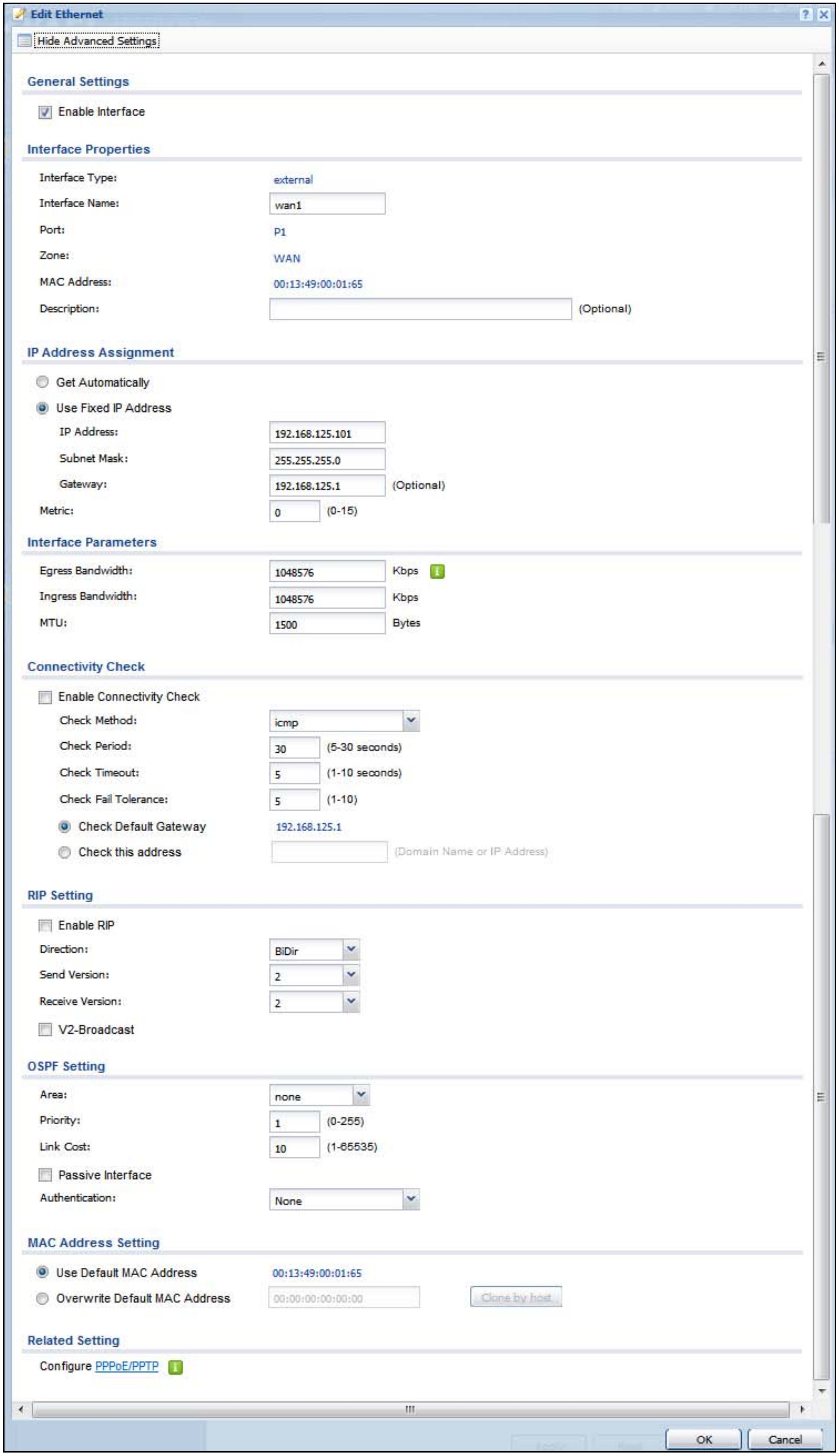
With RIP, you can use Ethernet interfaces to do the following things.

- Enable and disable RIP in the underlying physical port or port group.
- Select which direction(s) routing information is exchanged - The ISG50 can receive routing information, send routing information, or do both.
- Select which version of RIP to support in each direction - The ISG50 supports RIP-1, RIP-2, and both versions.
- Select the broadcasting method used by RIP-2 packets - The ISG50 can use subnet broadcasting or multicasting.

With OSPF, you can use Ethernet interfaces to do the following things.

- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The ISG50 can receive routing information, send routing information, or do both.
- Set the priority used to identify the DR or BDR if one does not exist.

Figure 172 Configuration > Network > Interface > Ethernet > Edit (WAN)



General Settings

☑ Enable Interface

Interface Properties

Interface Type: external
Interface Name: wan1
Port: P1
Zone: WAN
MAC Address: 00:13:49:00:01:65
Description: (Optional)

IP Address Assignment

○ Get Automatically
● Use Fixed IP Address
IP Address: 192.168.125.101
Subnet Mask: 255.255.255.0
Gateway: 192.168.125.1 (Optional)
Metric: 0 (0-15)

Interface Parameters

Egress Bandwidth: 1048576 Kbps
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes

Connectivity Check

☐ Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-30 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
● Check Default Gateway 192.168.125.1
○ Check this address (Domain Name or IP Address)

RIP Setting

☐ Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
☐ V2-Broadcast

OSPF Setting

Area: none
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
☐ Passive Interface
Authentication: None

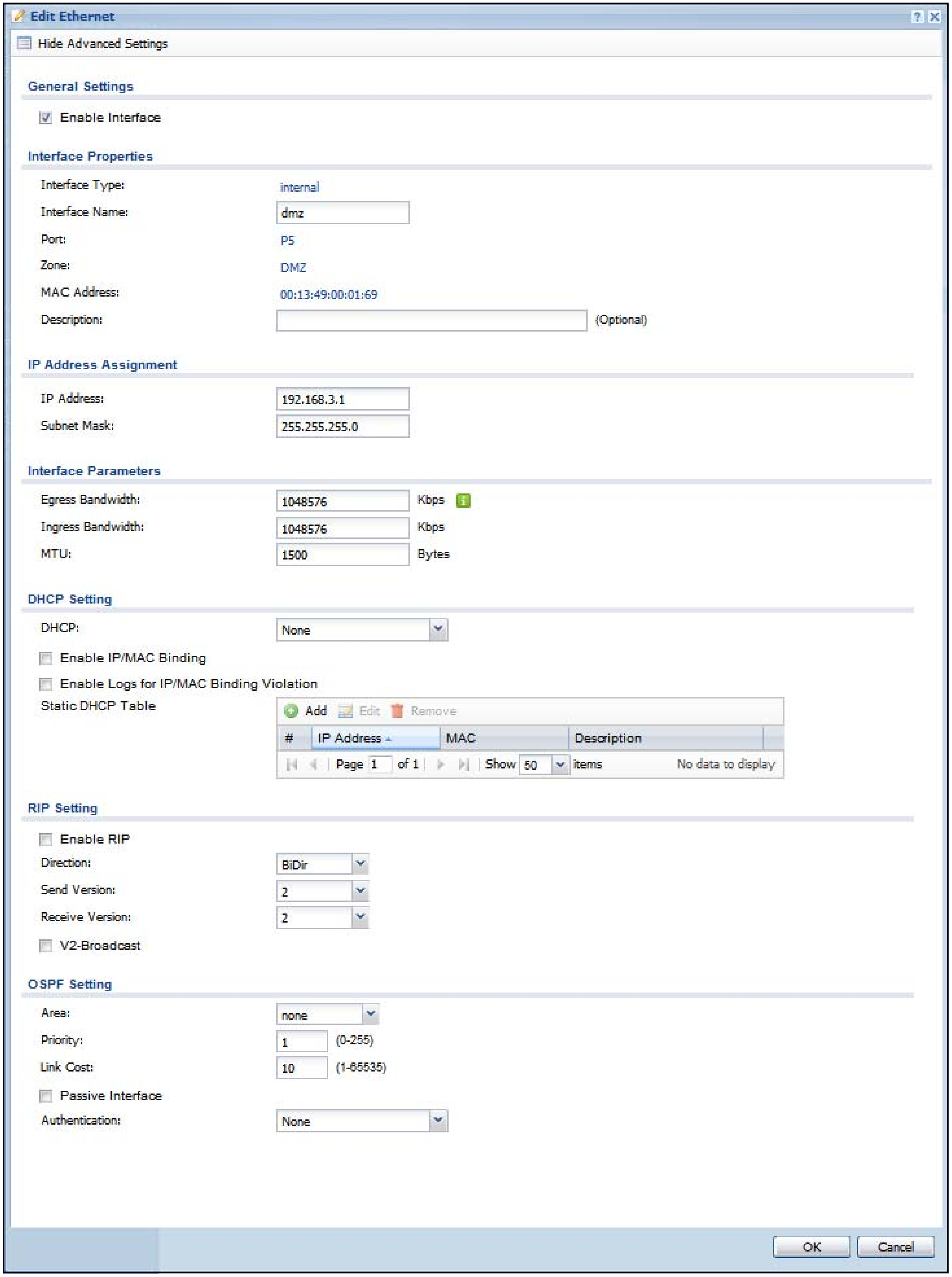
MAC Address Setting

● Use Default MAC Address 00:13:49:00:01:65
○ Overwrite Default MAC Address 00:00:00:00:00:00

Related Setting

Configure PPPoE/PPTP

Figure 173 Configuration > Network > Interface > Ethernet > Edit (DMZ)



General Settings

☑ Enable Interface

Interface Properties

Interface Type: internal

Interface Name: dmz

Port: P5

Zone: DMZ

MAC Address: 00:13:49:00:01:69

Description: (Optional)

IP Address Assignment

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Interface Parameters

Egress Bandwidth: 1048576 Kbps

Ingress Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

DHCP Setting

DHCP: None

☐ Enable IP/MAC Binding

☐ Enable Logs for IP/MAC Binding Violation

Static DHCP Table

Add Edit Remove

#	IP Address	MAC	Description

Page 1 of 1 Show 50 items No data to display

RIP Setting

☐ Enable RIP

Direction: BiDir

Send Version: 2

Receive Version: 2

☐ V2-Broadcast

OSPF Setting

Area: none

Priority: 1 (0-255)

Link Cost: 10 (1-65535)

☐ Passive Interface

Authentication: None

This screen's fields are described in the table below.

Table 65 Configuration > Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Type	This field is read-only. **internal** - is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ISG50 automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** - is for connecting to an external network (like the Internet). The ISG50 automatically adds this interface to the default WAN trunk.
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.
Zone	This is the zone to which this interface belongs. You use zones to apply security settings such as firewall and remote management.
MAC Address	This field is read-only. This is the MAC address that the Ethernet interface uses.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	These IP address fields configure an IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	This option appears when **Interface Properties** is **external**. Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	This option appears when **Interface Properties** is **external**. Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This option appears when **Interface Properties** is **external**. Enter the IP address of the gateway. The ISG50 sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	This option appears when **Interface Properties** is **external**. Enter the priority of the gateway (if any) on this interface. The ISG50 decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ISG50 uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ISG50 can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ISG50 can receive from the network through the interface. Allowed values are 0 - 1048576.

Table 65 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ISG50 divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	These fields appear when **Interface Properties** is **external**. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ISG50 stops routing to the gateway. The ISG50 resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ISG50 regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ISG50 regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ISG50 stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
DHCP Setting	These fields appear when **Interface Properties** is **Internal** or **General**.
DHCP	Select what type of DHCP service the ISG50 provides to the network. Choices are: **None** - the ISG50 does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ISG50 routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ISG50 assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ISG50 is the DHCP server for the network.
	The following fields appear if the ISG50 is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	The following fields appear if the ISG50 is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ISG50 begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP Table**. If this field is blank, the **Pool Size** must also be blank. In this case, the ISG50 can assign every IP address allowed by the interface’s IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface’s IP address.

Table 65 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ISG50 can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ISG50 can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **ISG50** - the DHCP clients use the IP address of this interface and the ISG50 works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire. **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ISG50 generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the ISG50 assigns to computers connected to the interface. Otherwise, the ISG50 assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 15.2 on page 302 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.

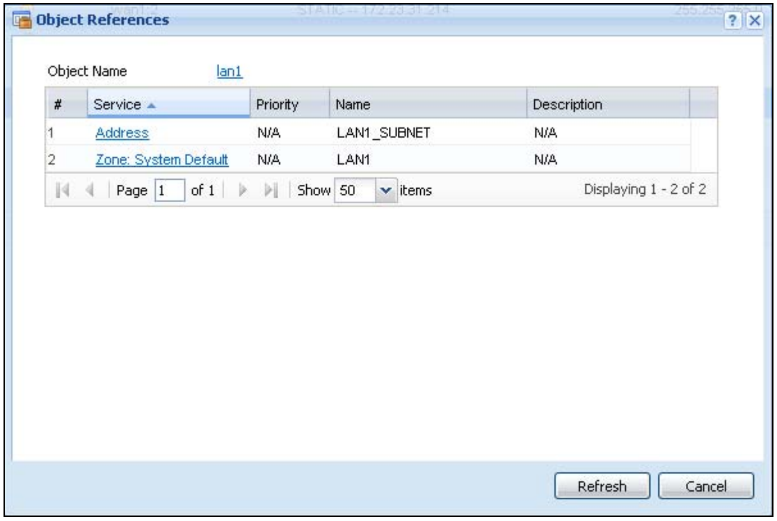
Table 65 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ISG50 uses multicasting.
OSPF Setting	See Section 15.3 on page 304 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to eight characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MAC Address Setting	This section appears when **Interface Properties** is **External** or **General**. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the ISG50 uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click **Clone by host** and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Related Setting	
Configure PPPoE/PPTP	Click **PPPoE/PPTP** if this interface's Internet connection uses PPPoE or PPTP.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

12.3.2 Object References

When a configuration screen includes an **Object References** icon, select a configuration object and click **Object References** to open the **Object References** screen. This screen displays which configuration settings reference the selected object. The fields shown vary with the type of object.

Figure 174 Object References



Object Name lan1

#	Service	Priority	Name	Description
1	Address	N/A	LAN1_SUBNET	N/A
2	Zone: System Default	N/A	LAN1	N/A

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

The following table describes labels that can appear in this screen.

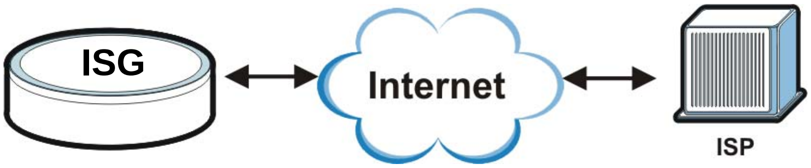
Table 66 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise **N/A** displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click **Cancel** to close the screen.

12.4 PPP Interfaces

Use PPPoE/PPTP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

Figure 175 Example: PPPoE/PPTP Interfaces


ISG
Internet
ISP

PPPoE/PPTP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP interfaces and other interfaces.

- You must also configure an ISP account object for the PPPoE/PPTP interface to use.

  Each ISP account specifies the protocol (PPPoE or PPTP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP interface. You should not have to change any network policies.

- You do not set up the subnet mask or gateway.

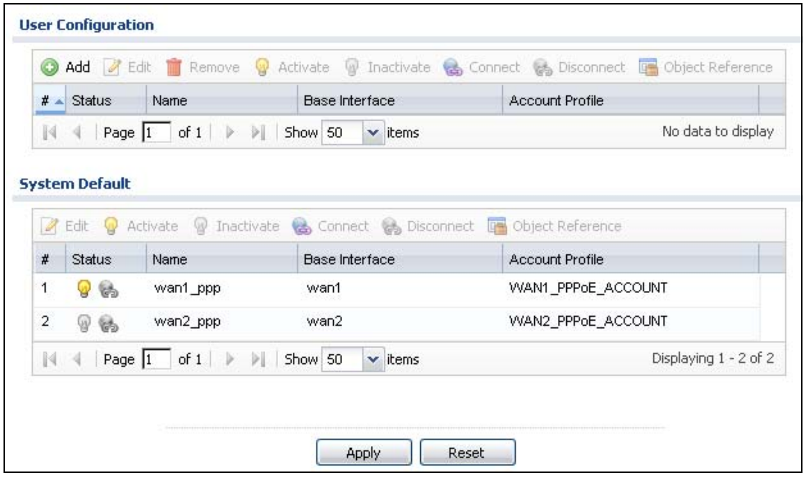
  PPPoE/PPTP interfaces are interfaces between the ISG50 and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the ISG50 always treats the ISP as a gateway.

At the time of writing, it is possible to set up the IP address of the gateway (ISP) using CLI commands but not in the Web Configurator.

12.4.1 PPP Interface Summary

This screen lists every PPPoE/PPTP interface. To access this screen, click **Configuration > Network** > **Interface** > **PPP**.

Figure 176 Configuration > Network > Interface > PPP


User Configuration
Add
Edit
Remove
Activate
Inactivate
Connect
Disconnect
Object Reference
Page 1 of 1
Show 50 items
System Default
Edit
Activate
Inactivate
Connect
Disconnect
Object Reference
Page 1 of 1
Show 50 items
Displaying 1 - 2 of 2
Apply
Reset

#	Status	Name	Base Interface	Account Profile

No data to display

#	Status	Name	Base Interface	Account Profile
1		wan1_ppp	wan1	WAN1_PPPoE_ACCOUNT
2		wan2_ppp	wan2	WAN2_PPPoE_ACCOUNT

Each field is described in the table below.

Table 67 Configuration > Network > Interface > PPP

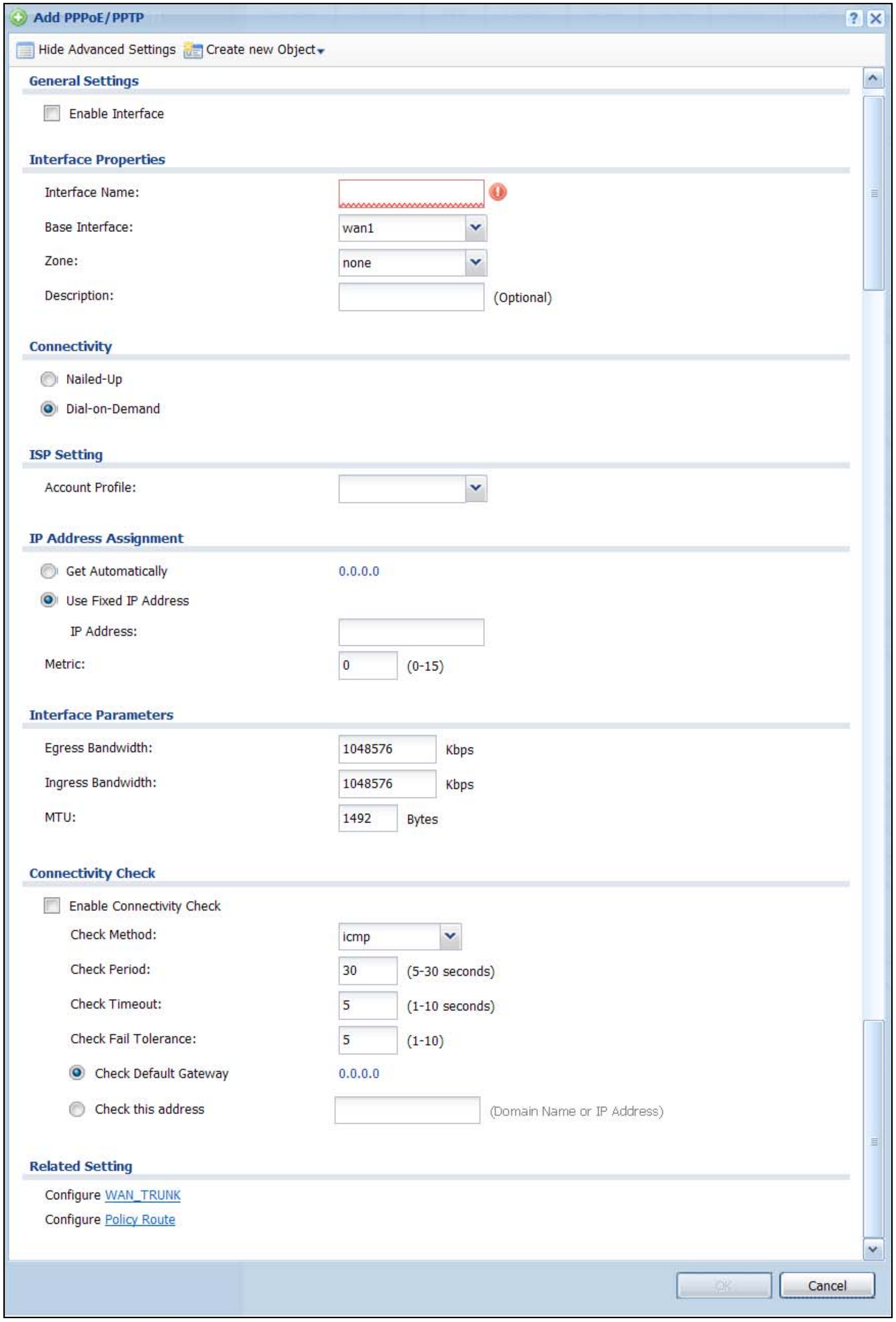
LABEL	DESCRIPTION
User Configuration / System Default	The ISG50 comes with the (non-removable) **System Default** PPP interfaces pre-configured. You can create (and delete) **User Configuration** PPP interfaces.
Add	Click this to create a new user-configured PPP interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured PPP interface, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection for a **Dial-on-Demand** PPPoE/PPTP interface.
Disconnect	To disconnect an interface, select it and click **Disconnect**. You might use this in testing the interface.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.4.2 PPP Interface Add or Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lets you configure a PPPoE or PPTP interface. To access this screen, click the **Add** icon or an **Edit** icon in the PPP Interface screen.

Figure 177 Configuration > Network > Interface > PPP > Add



General Settings

☐ Enable Interface

Interface Properties

Interface Name:

Base Interface: wan1

Zone: none

Description: (Optional)

Connectivity

○ Nailed-Up

● Dial-on-Demand

ISP Setting

Account Profile:

IP Address Assignment

○ Get Automatically 0.0.0.0

● Use Fixed IP Address

IP Address:

Metric: 0 (0-15)

Interface Parameters

Egress Bandwidth: 1048576 Kbps

Ingress Bandwidth: 1048576 Kbps

MTU: 1492 Bytes

Connectivity Check

☐ Enable Connectivity Check

Check Method: icmp

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

● Check Default Gateway 0.0.0.0

○ Check this address (Domain Name or IP Address)

Related Setting

Configure WAN_TRUNK

Configure Policy Route

Each field is explained in the following table.

Table 68 Configuration > Network > Interface > PPP > Add

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	

Table 68 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Base Interface	Select the interface upon which this PPP interface is built. Note: Multiple PPP interfaces can use the same base interface.
Zone	Select the zone to which you want the PPP interface to belong. The zone determines the security settings the ISG50 uses for the interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the PPPoE/PPTP connection should always be up. Clear this to have the ISG50 establish the PPPoE/PPTP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time.
Dial-on-Demand	Select this to have the ISG50 establish the PPPoE/PPTP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available.
ISP Setting	
Account Profile	Select the ISP account that this PPPoE/PPTP interface uses. The drop-down box lists ISP accounts by name. Use **Create new Object** if you need to configure a new ISP account (see Chapter 51 on page 661 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	Click **Show Advanced Settings** to display more settings. Click **Hide Advanced Settings** to display fewer settings.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The ISG50 decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ISG50 uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ISG50 can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ISG50 can receive from the network through the interface. Allowed values are 0 - 1048576.

Table 68 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ISG50 divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ISG50 stops routing to the gateway. The ISG50 resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ISG50 regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ISG50 regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ISG50 stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

12.5 Cellular Configuration Screen (3G)

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

Note: The actual data rate you obtain varies depending on the 3G card you use, the signal strength to the service provider's base station, and so on.

You can configure how the ISG50's 3G device connects to a network (refer to Section 12.5.1 on page 253):

- You can set the 3G device to connect only to the home network, which is the network to which you are originally subscribed.
- You can set the 3G device to connect to other networks if the signal strength of the home network is too low or it is unavailable.

Aside from selecting the 3G network, the 3G card may also select an available 2.5G or 2.75G network automatically. See the following table for a comparison between 2G, 2.5G, 2.75G and 3G of wireless technologies.

Table 69 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	**CDMA-BASED**	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		Fast

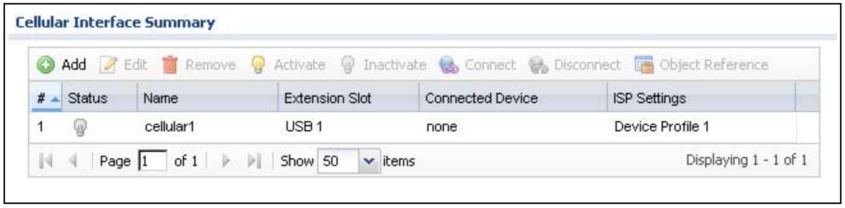
[A] The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

To change your 3G WAN settings, click **Configuration > Network > Interface** > **Cellular**.

Note: Install (or connect) a compatible 3G USB to use a cellular connection.

Note: The WAN IP addresses of a ISG50 with multiple WAN interfaces must be on different subnets.

Figure 178 Configuration > Network > Interface > Cellular



#	Status	Name	Extension Slot	Connected Device	ISP Settings
1	💡	cellular1	USB 1	none	Device Profile 1

The following table describes the labels in this screen.

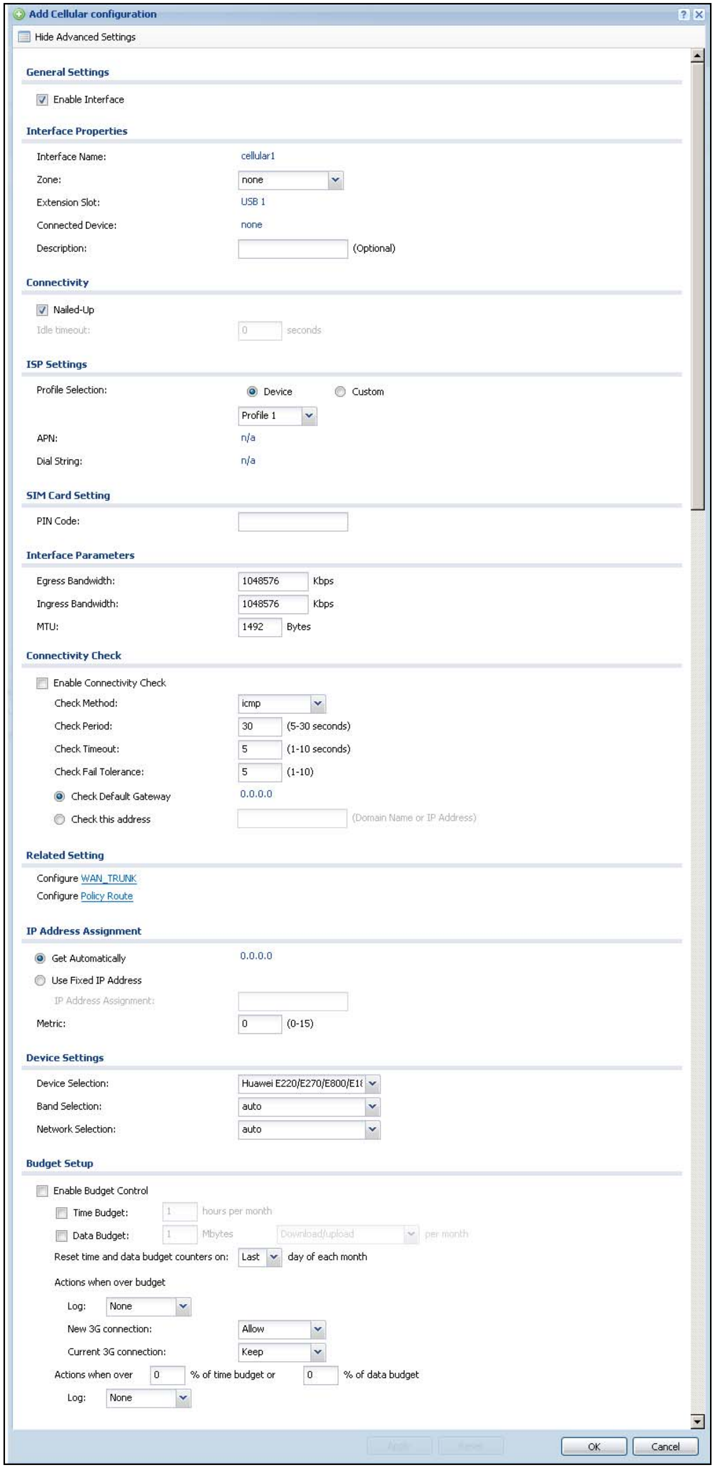
Table 70 Configuration > Network > Interface > Cellular

LABEL	DESCRIPTION
Add	Click this to create a new cellular interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection.
Disconnect	To disconnect an interface, select it and click **Disconnect**. You might use this in testing the interface.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the name of the cellular card.
ISP Settings	This field displays the profile of ISP settings that this cellular interface is set to use.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.5.1 Cellular Add/Edit Screen

To change your 3G settings, click **Configuration > Network > Interface** > **Cellular > Add** (or **Edit**). In the pop-up window that displays, select the slot that you want to configure. The following screen displays.

Figure 179 Configuration > Network > Interface > Cellular > Add



General Settings

☑ Enable Interface

Interface Properties

Interface Name: cellular1
Zone: none
Extension Slot: USB 1
Connected Device: none
Description: (Optional)

Connectivity

☑ Nailed-Up
Idle timeout: 0 seconds

ISP Settings

Profile Selection: ● Device ○ Custom
Profile 1
APN: n/a
Dial String: n/a

SIM Card Setting

PIN Code:

Interface Parameters

Egress Bandwidth: 1048576 Kbps
Ingress Bandwidth: 1048576 Kbps
MTU: 1492 Bytes

Connectivity Check

☐ Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-30 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
● Check Default Gateway 0.0.0.0
○ Check this address (Domain Name or IP Address)

Related Setting

Configure WAN_TRUNK
Configure Policy Route

IP Address Assignment

● Get Automatically 0.0.0.0
○ Use Fixed IP Address
IP Address Assignment:
Metric: 0 (0-15)

Device Settings

Device Selection: Huawei E220/E270/E800/E1
Band Selection: auto
Network Selection: auto

Budget Setup

☐ Enable Budget Control
☐ Time Budget: 1 hours per month
☐ Data Budget: 1 Mbytes Download/upload per month
Reset time and data budget counters on: Last day of each month
Actions when over budget
Log: None
New 3G connection: Allow
Current 3G connection: Keep
Actions when over 0 % of time budget or 0 % of data budget
Log: None

The following table describes the labels in this screen.

Table 71 Configuration > Network > Interface > Cellular > Add

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this option to turn on this interface.
Interface Properties	
Interface Name	Select a name for the interface.
Zone	Select the zone to which you want the cellular interface to belong. The zone determines the security settings the ISG50 uses for the interface.
Extension Slot	This is the USB slot that you are configuring for use with a 3G card.
Connected Device	This displays the manufacturer and model name of your 3G card if you inserted one in the ISG50. Otherwise, it displays **none**.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the connection should always be up. Clear this to have the ISG50 to establish the connection only when there is traffic. You might not nail up the connection if there is little traffic through the interface or if it costs money to keep the connection available.
Idle timeout	This value specifies the time in seconds (0~360) that elapses before the ISG50 automatically disconnects from the ISP's server. Zero disables the idle timeout.
ISP Settings	
Profile Selection	Select **Device** to use one of the 3G device's profiles of device settings. Then select the profile (use **Profile 1** unless your ISP instructed you to do otherwise). Select **Custom** to configure your device settings yourself.
APN	This field is read-only if you selected **Device** in the profile selection. Select **Custom** in the profile selection to be able to manually input the APN (Access Point Name) provided by your service provider. This field applies with a GSM or HSDPA 3G card. Enter the APN from your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 63 ASCII printable characters. Spaces are allowed.
Dial String	Enter the dial string if your ISP provides a string, which would include the APN, to initialize the 3G card. You can enter up to 63 ASCII printable characters. Spaces are allowed. This field is available only when you insert a GSM 3G card.
Authentication Type	The ISG50 supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **None:** No authentication for outgoing calls. **CHAP** - Your ISG50 accepts CHAP requests only. **PAP** - Your ISG50 accepts PAP requests only.

Table 71 Configuration > Network > Interface > Cellular > Add (continued)

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>User Name</td><td>This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection. If this field is configurable, enter the user name for this 3G card exactly as the service provider gave it to you.
You can use 1 ~ 64 alphanumeric and <code>#:%-_@$./</code> characters. The first character must be alphanumeric or <code>-_@$./</code>. Spaces are not allowed.</td></tr>
<tr><td>Password</td><td>This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection and the password is included in the 3G card’s profile. If this field is configurable, enter the password for this SIM card exactly as the service provider gave it to you.
You can use 0 ~ 63 alphanumeric and <code>`~!@#$%^&*()_-+={}|;:'<,>./</code> characters. Spaces are not allowed.</td></tr>
<tr><td>Retype to Confirm</td><td>This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection and the password is included in the 3G card’s profile. If this field is configurable, re-enter the password for this SIM card exactly as the service provider gave it to you.</td></tr>
<tr><td>SIM Card Setting</td><td></td></tr>
<tr><td>PIN Code</td><td>This field displays with a GSM or HSDPA 3G card. A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card.
Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet.
If your ISP disabled PIN code authentication, enter an arbitrary number.</td></tr>
<tr><td>Interface Parameters</td><td></td></tr>
<tr><td>Egress Bandwidth</td><td>Enter the maximum amount of traffic, in kilobits per second, the ISG50 can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.</td></tr>
<tr><td>Ingress Bandwidth</td><td>This is reserved for future use.
Enter the maximum amount of traffic, in kilobits per second, the ISG50 can receive from the network through the interface. Allowed values are 0 - 1048576.</td></tr>
<tr><td>MTU</td><td>Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ISG50 divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.</td></tr>
<tr><td>Connectivity Check</td><td>The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ISG50 stops routing to the gateway. The ISG50 resumes routing to the gateway the first time the gateway passes the connectivity check.</td></tr>
<tr><td>Enable Connectivity Check</td><td>Select this to turn on the connection check.</td></tr>
<tr><td>Check Method</td><td>Select the method that the gateway allows.
Select icmp to have the ISG50 regularly ping the gateway you specify to make sure it is still available.
Select tcp to have the ISG50 regularly perform a TCP handshake with the gateway you specify to make sure it is still available.</td></tr>
<tr><td>Check Period</td><td>Enter the number of seconds between connection check attempts.</td></tr>
<tr><td>Check Timeout</td><td>Enter the number of seconds to wait for a response before the attempt is a failure.</td></tr>
</table>

Table 71 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
Check Fail Tolerance	Enter the number of consecutive failures before the ISG50 stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the policy route summary screen where you can configure a policy route to override the default routing and SNAT behavior for the interface.
IP Address Assignment	
Get Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address Assignment	Enter the cellular interface's WAN IP address in this field if you selected **Use Fixed IP Address**.
Metric	Enter the priority of the gateway (if any) on this interface. The ISG50 decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ISG50 uses the one that was configured first.
Device Settings	
Device Selection	Select the 3G card to use with this entry or select **auto** to have the ISG50 automatically detect the type of card.
Band Selection	This field appears if you selected a 3G device that allows you to select the type of network to use. Select the type of 3G service for your 3G connection. If you are unsure what to select, check with your 3G service provider to find the 3G service available to you in your region. Select **auto** to have the card connect to an available network. Choose this option if you do not know what networks are available. You may want to manually specify the type of network to use if you are charged differently for different types of network or you only have one type of network available to you. Select **GPRS / EDGE (GSM) only** to have this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to select this so the ISG50 does not spend time looking for a WCDMA network. Select **UMTS / HSDPA (WCDMA) only** to have this interface only use a 3G or 3.5G network (respectively). You may want to do this if you want to make sure the interface does not use the GSM network.

Table 71 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
Network Selection	Home network is the network to which you are originally subscribed. Select **Home** to have the 3G device connect only to the home network. If the home network is down, the ISG50's 3G Internet connection is also unavailable. Select **Auto** (Default) to allow the 3G device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another 3G base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
Budget Setup	
Enable Budget Control	Select this to set a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The ISG50 takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the 3G connection can be used within one month. If you change the value after you configure and enable budget control, the ISG50 resets the statistics.
Data Budget	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. Select **Download** to set a limit on the downstream traffic (from the ISP to the ISG50). Select **Upload** to set a limit on the upstream traffic (from the ISG50 to the ISP). Select **Download/Upload** to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the ISG50 resets the statistics.
Reset time and data budget counters on	Select the date on which the ISG50 resets the budget every month. If the date you selected is not available in a month, such as 30th or 31th, the ISG50 resets the budget on the last day of the month.
Reset time and data budget counters	This button is available only when you enable budget control in this screen. Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection’s full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.
Actions when over budget	Specify the actions the ISG50 takes when the time or data limit is exceeded.
Log	Select **None** to not create a log, **Log** to create a log, or **Log-alert** to create an alert log. If you select **Log** or **Log-alert** you can also select **recurring every** to have the ISG50 send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
New 3G connection	Select **Allow** to permit new 3G connections or **Disallow** to drop/block new 3G connections.
Current 3G connection	Select **Keep** to maintain an existing 3G connection or **Drop** to disconnect it. You cannot set **New 3G connection** to **Allow** and **Current 3G connection** to **Drop** at the same time. If you set **New 3G connection** to **Disallow** and **Current 3G connection** to **Keep**, the ISG50 allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.

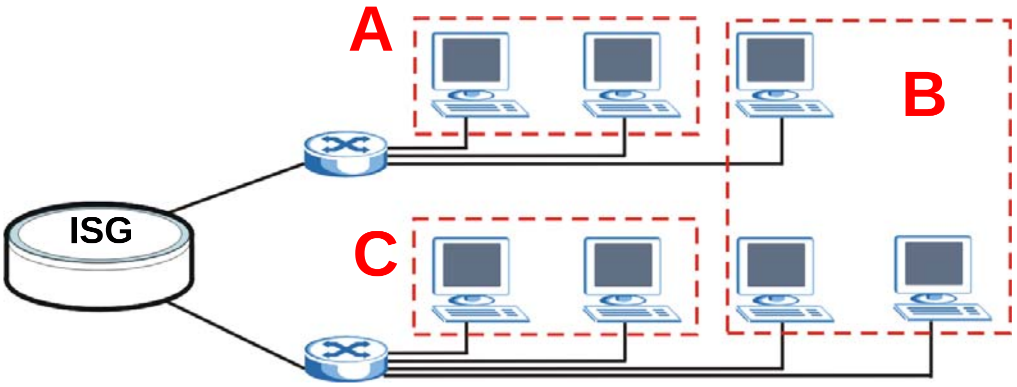
Table 71 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
Actions when over % of time budget or % of data budget	Specify the actions the ISG50 takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the ISG50 resets the statistics. Select **None** to not create a log when the ISG50 takes this action, **Log** to create a log, or **Log-alert** to create an alert log. If you select **Log** or **Log-alert** you can also select **recurring every** to have the ISG50 send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

12.6 VLAN Interfaces

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

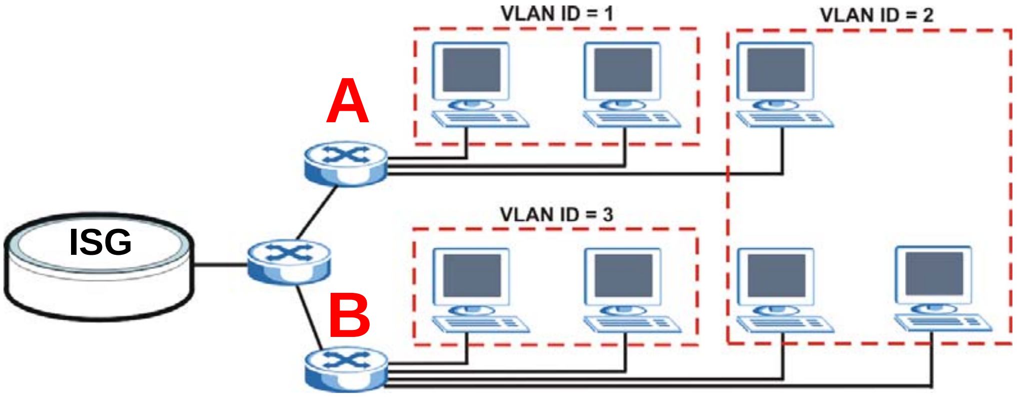
Figure 180 Example: Before VLAN



In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Alternatively, you can divide the physical networks into three VLANs.

Figure 181 Example: After VLAN



Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.
- Better manageability - You can align network policies more appropriately for users. For example, you can create different rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

VLAN Interfaces Overview

In the ISG50, each VLAN is called a VLAN interface. As a router, the ISG50 routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

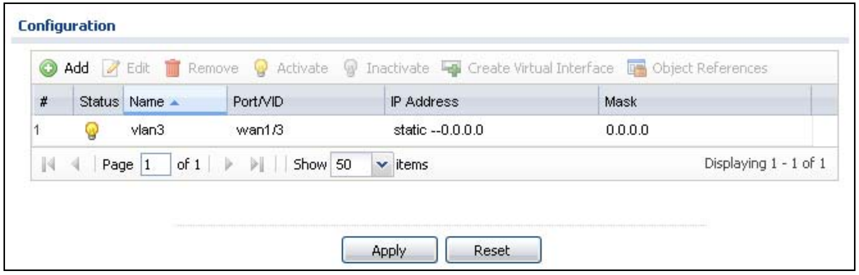
Note: Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

12.6.1 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. To access this screen, click **Configuration > Network > Interface** > **VLAN**.

Figure 182 Configuration > Network > Interface > VLAN



#	Status	Name	Port/VID	IP Address	Mask
1	💡	vlan3	wan1/3	static --0.0.0.0	0.0.0.0

Each field is explained in the following table.

Table 72 Configuration > Network > Interface > VLAN

LABEL	DESCRIPTION
Add	Click this to create a new VLAN interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click **Create Virtual Interface**.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
Port/VID	For VLAN interfaces, this field displays • the Ethernet interface on which the VLAN interface is created • the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.

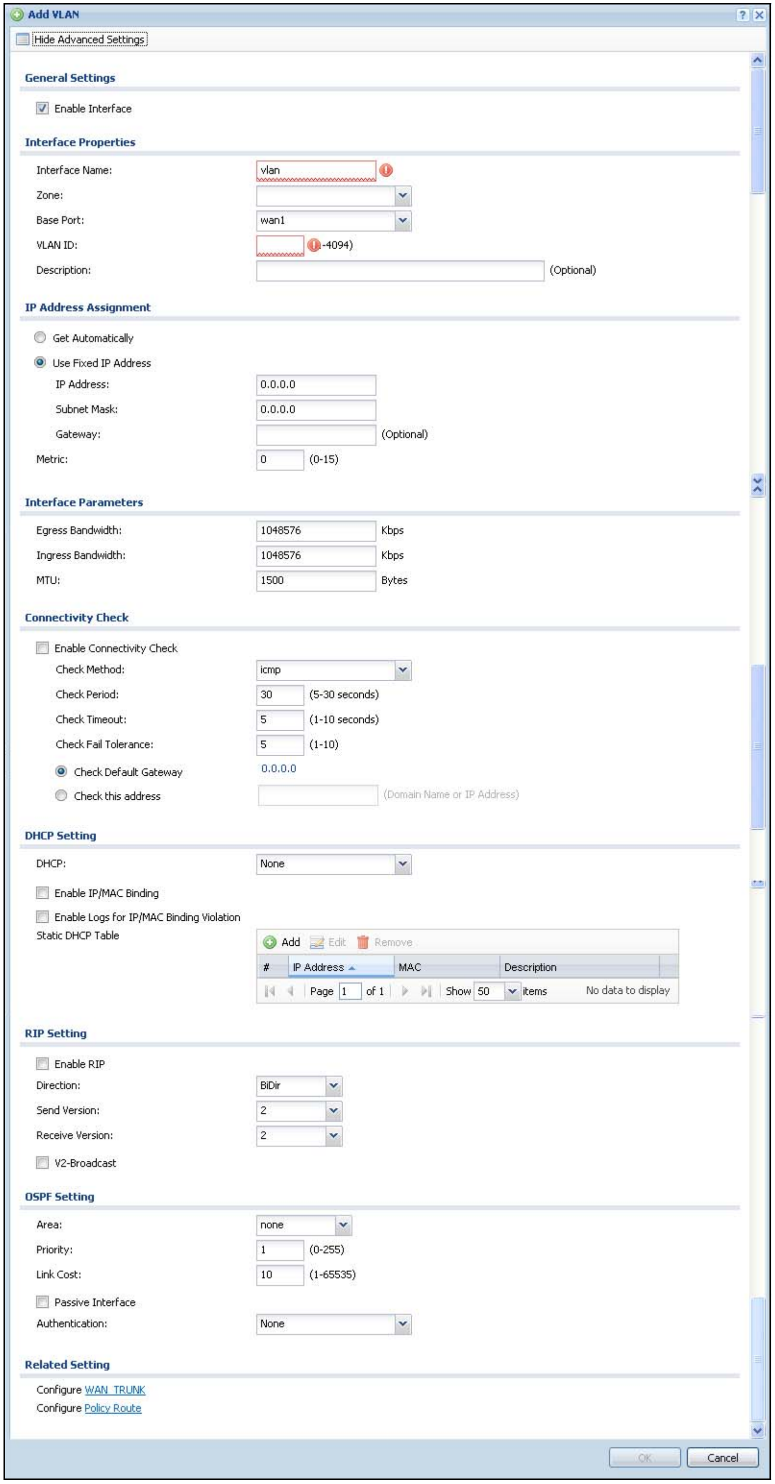
Table 72 Configuration > Network > Interface > VLAN (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.6.2 VLAN Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each VLAN interface. To access this screen, click the **Add** icon at the top of the **Add** column or click an **Edit** icon next to a VLAN interface in the **VLAN Summary** screen. The following screen appears.

Figure 183 Configuration > Network > Interface > VLAN > Edit



General Settings

☑ Enable Interface

Interface Properties

Interface Name: vlan

Zone:

Base Port: wan1

VLAN ID: -4094)

Description: (Optional)

IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0-15)

Interface Parameters

Egress Bandwidth: 1048576 Kbps

Ingress Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

Connectivity Check

☐ Enable Connectivity Check

Check Method: icmp

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

● Check Default Gateway 0.0.0.0

○ Check this address (Domain Name or IP Address)

DHCP Setting

DHCP: None

☐ Enable IP/MAC Binding

☐ Enable Logs for IP/MAC Binding Violation

Static DHCP Table

Add Edit Remove

#	IP Address	MAC	Description

Page 1 of 1 Show 50 items No data to display

RIP Setting

☐ Enable RIP

Direction: BiDir

Send Version: 2

Receive Version: 2

☐ V2-Broadcast

OSPF Setting

Area: none

Priority: 1 (0-255)

Link Cost: 10 (1-65535)

☐ Passive Interface

Authentication: None

Related Setting

Configure WAN_TRUNK

Configure Policy Route

Each field is explained in the following table.

Table 73 Configuration > Network > Interface > VLAN > Edit

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this to turn this interface on. Clear this to disable this interface.
Interface Properties	
Interface Name	This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. See for the total number of VLANs you can configure on the ISG50. For example, vlan0, vlan8, and so on.
Zone	Select the zone to which the VLAN interface belongs.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ISG50 sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ISG50 decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ISG50 uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ISG50 can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ISG50 can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ISG50 divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.

Table 73 Configuration > Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
Connectivity Check	The ISG50 can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ISG50 stops routing to the gateway. The ISG50 resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ISG50 regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ISG50 regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ISG50 stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
DHCP Setting	The DHCP settings are available for the OPT, LAN and DMZ interfaces.
DHCP	Select what type of DHCP service the ISG50 provides to the network. Choices are: **None** - the ISG50 does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ISG50 routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ISG50 assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ISG50 is the DHCP server for the network.
	The following fields appear if the ISG50 is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	The following fields appear if the ISG50 is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ISG50 begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ISG50 can assign every IP address allowed by the interface’s IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface’s IP address.

Table 73 Configuration > Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ISG50 can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ISG50 can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **ISG50** - the DHCP clients use the IP address of this interface and the ISG50 works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Enable IP/MAC Binding	Select this option to have the ISG50 enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ISG50 generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the ISG50 assigns to computers connected to the interface. Otherwise, the ISG50 assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 15.2 on page 302 for more information about RIP.
Enable RIP	Select this to enable RIP on this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.

Table 73 Configuration > Network > Interface > VLAN > Edit (continued)

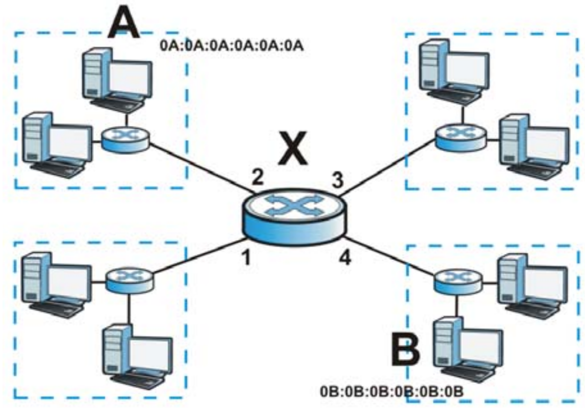
LABEL	DESCRIPTION
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ISG50 uses multicasting.
OSPF Setting	See Section 15.3 on page 304 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to eight characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this VLAN.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

12.7 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge X connects four network segments.



When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

Table 74 Example: Bridge Table After Computer A Sends a Packet to Computer B

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

Table 75 Example: Bridge Table After Computer B Responds to Computer A

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2
0B:0B:0B:0B:0B:0B	4

Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the ISG50's interface for the resulting network.

The ISG50 can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole ISG50 as a transparent bridge, add all of the ISG50's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the ISG50 removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between lan1 and vlan1.

Table 76 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	lan1
210.211.1.0/24	lan1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz

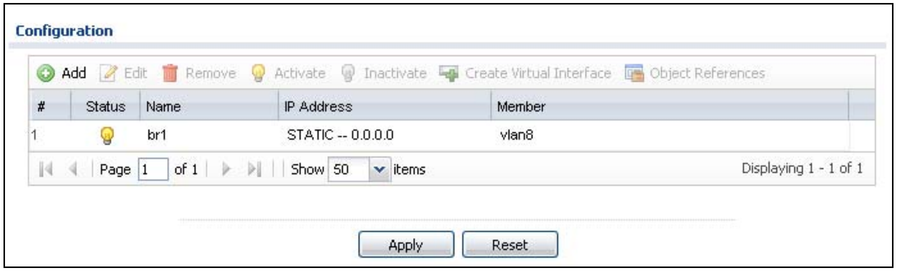
IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz
250.250.250.0/23	br0

In this example, virtual Ethernet interface lan1:1 is also removed from the routing table when lan1 is added to br0. Virtual interfaces are automatically added to or remove from a bridge interface when the underlying interface is added or removed.

12.7.1 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. To access this screen, click **Configuration > Network > Interface** > **Bridge**.

Figure 184 Configuration > Network > Interface > Bridge



#	Status	Name	IP Address	Member
1	💡	br1	STATIC -- 0.0.0.0	vlan8

Each field is described in the following table.

Table 77 Configuration > Network > Interface > Bridge

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click **Create Virtual Interface**.

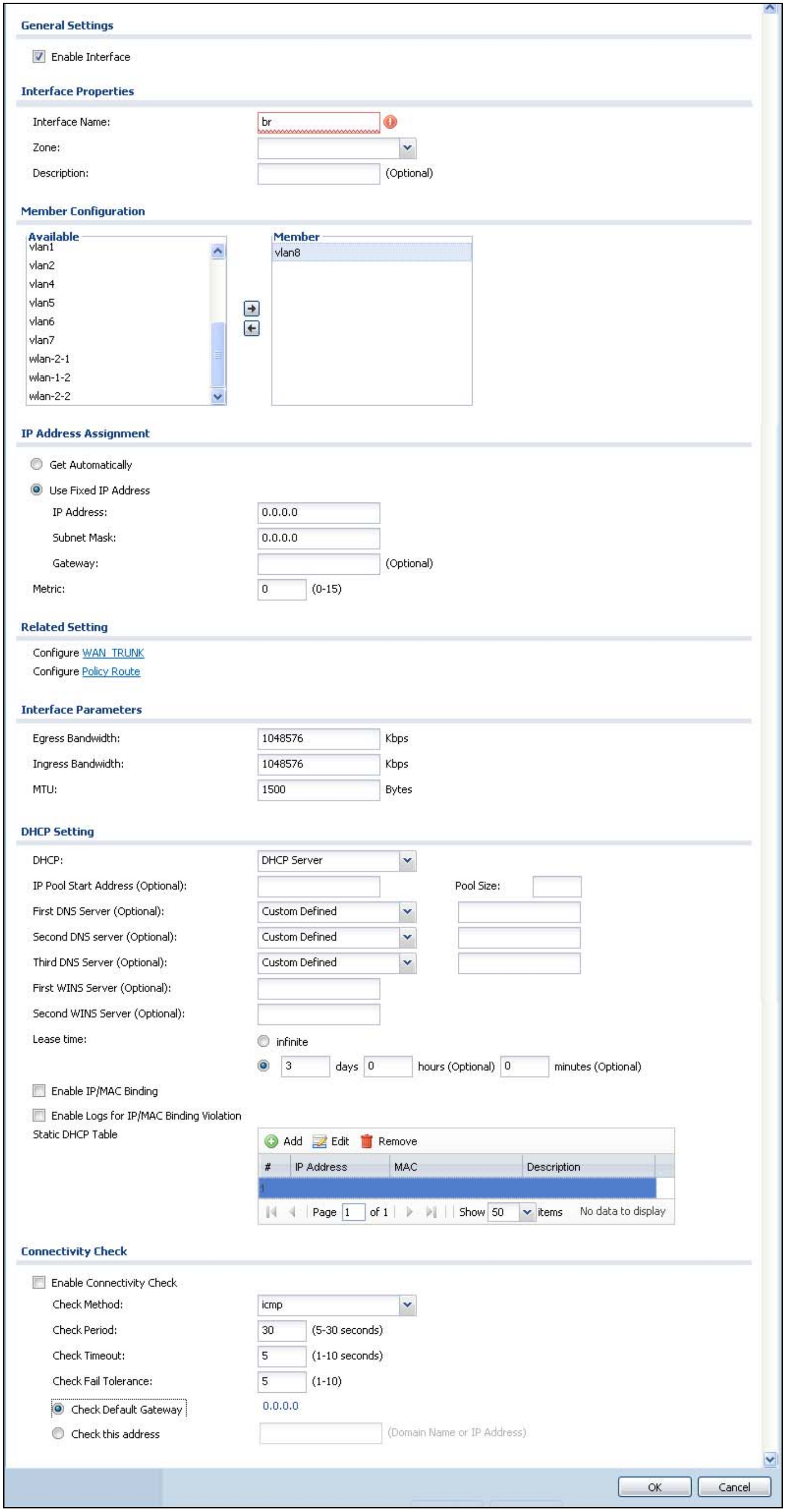
Table 77 Configuration > Network > Interface > Bridge (continued)

LABEL	DESCRIPTION
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.7.2 Bridge Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each bridge interface. To access this screen, click the **Add** icon at the top of the **Add** column in the **Bridge Summary** screen, or click an **Edit** icon in the **Bridge Summary** screen. The following screen appears.

Figure 185 Configuration > Network > Interface > Bridge > Add



General Settings

☑ Enable Interface

Interface Properties

Interface Name: br

Zone:

Description: (Optional)

Member Configuration

Available: vlan1, vlan2, vlan4, vlan5, vlan6, vlan7, wlan-2-1, wlan-1-2, wlan-2-2

Member: vlan8

IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0-15)

Related Setting

Configure WAN_TRUNK

Configure Policy Route

Interface Parameters

Egress Bandwidth: 1048576 Kbps

Ingress Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

DHCP Setting

DHCP: DHCP Server

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional): Custom Defined

Second DNS server (Optional): Custom Defined

Third DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):

Lease time: ○ infinite

● 3 days 0 hours (Optional) 0 minutes (Optional)

☐ Enable IP/MAC Binding

☐ Enable Logs for IP/MAC Binding Violation

Static DHCP Table

#	IP Address	MAC	Description

Connectivity Check

☐ Enable Connectivity Check

Check Method: icmp

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

● Check Default Gateway 0.0.0.0

○ Check this address (Domain Name or IP Address)

Each field is described in the table below.

Table 78 Configuration > Network > Interface > Bridge > Edit

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on.
Zone	Select the zone to which the interface is to belong. You use zones to apply security settings such as firewall and remote management.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Member Configuration	
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the **>>** arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the **<<** arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ISG50 sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ISG50 decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ISG50 uses the one that was configured first.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.

Table 78 Configuration > Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ISG50 can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ISG50 can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ISG50 divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Setting	
DHCP	Select what type of DHCP service the ISG50 provides to the network. Choices are: **None** - the ISG50 does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ISG50 routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ISG50 assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ISG50 is the DHCP server for the network.
	The following fields appear if the ISG50 is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	The following fields appear if the ISG50 is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ISG50 begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ISG50 can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ISG50 can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ISG50 can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **ISG50** - the DHCP clients use the IP address of this interface and the ISG50 works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.

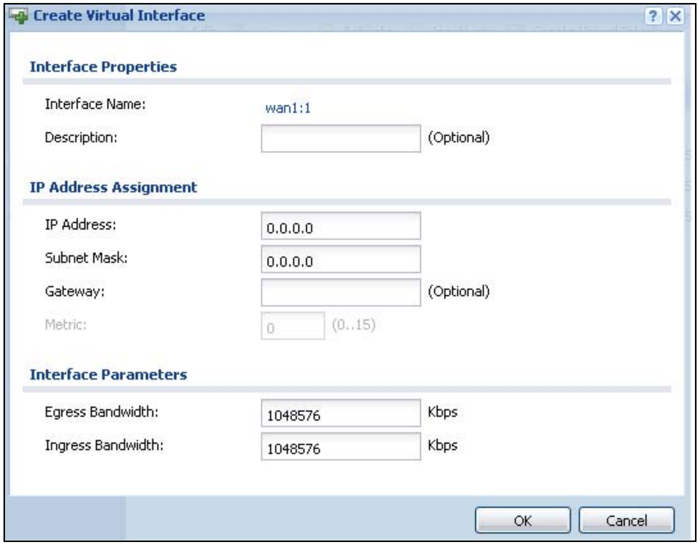
Table 78 Configuration > Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ISG50 generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the ISG50 assigns to computers connected to the interface. Otherwise, the ISG50 assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ISG50 stops routing to the gateway. The ISG50 resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ISG50 regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ISG50 regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ISG50 stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

12.7.3 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click an **Add** icon next to an Ethernet interface, VLAN interface, or bridge interface in the respective interface summary screen.

Figure 186 Virtual Interface Add



Create Virtual Interface

Interface Properties

Interface Name: wan1:1
Description: (Optional)

IP Address Assignment

IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway: (Optional)
Metric: 0 (0..15)

Interface Parameters

Egress Bandwidth: 1048576 Kbps
Ingress Bandwidth: 1048576 Kbps

Each field is described in the table below.

Table 79 Virtual Interface Add

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The ISG50 sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ISG50 decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ISG50 uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ISG50 can send through the interface to the network. Allowed values are 0 - 1048576.

Table 79 Virtual Interface Add (continued)

LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ISG50 can receive from the network through the interface. Allowed values are 0 - 1048576.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

12.8 Interface Technical Reference

Here is more detailed information about interfaces on the ISG50.

IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

Figure 187 Example: Entry in the Routing Table Derived from Interfaces

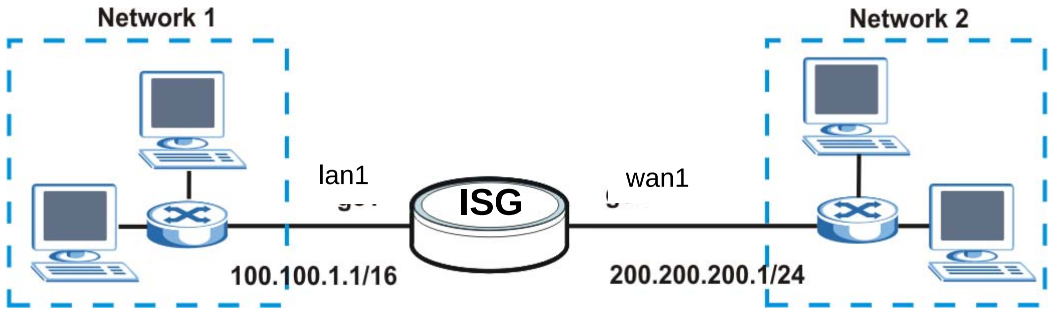


Table 80 Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	lan1
200.200.200.1/24	wan1

For example, if the ISG50 gets a packet with a destination address of 100.100.25.25, it routes the packet to interface lan1. If the ISG50 gets a packet with a destination address of 200.200.200.200, it routes the packet to interface wan1.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the ISG50 gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the ISG50 should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on wan2. In this case, the ISG50 creates the following entry in the routing table.

Table 81 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the ISG50 uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the ISG50 uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

Interface Parameters

The ISG50 restricts the amount of traffic into and out of the ISG50 through each interface.

- Egress bandwidth sets the amount of traffic the ISG50 sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the ISG50 allows in through the interface from the network.[1]

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The ISG50 also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the ISG50 divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

---

[1] At the time of writing, the ISG50 does not support ingress bandwidth management.

In the ISG50, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the ISG50's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

  Table 82 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

  The ISG50 cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the ISG50 cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the ISG50 cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

  If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See IP Address Assignment on page 276.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 276.
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecure TCP/IP environments. It sets up two sessions.

1. The first one runs on TCP port 1723. It is used to start and manage the second one.
2. The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

13

Trunks

13.1 Overview

Use trunks for WAN traffic load balancing to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

Maybe you have two Internet connections with different bandwidths. You could set up a trunk that uses spillover or weighted round robin load balancing so time-sensitive traffic (like video) usually goes through the higher-bandwidth interface. For other traffic, you might want to use least load first load balancing to even out the distribution of the traffic load.

Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routes and trunks to have traffic for your European branch office primarily use ISP A and traffic for your Australian branch office primarily use ISP B.

Or maybe one of the ISG50's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You can use policy routing to send the VoIP traffic through a trunk with the interface connected to the VoIP service provider set to active and another interface (connected to another ISP) set to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface’s connection is up.

13.1.1 What You Can Do in this Chapter

- Use the **Trunk** summary screen (Section 13.2 on page 285) to configure link sticking and view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the **Trunk Edit** screen (Section 13.3 on page 287) to configure which interfaces belong to each trunk and the load balancing algorithm each trunk uses.

13.1.2 What You Need to Know

- Add WAN interfaces to trunks to have multiple connections share the traffic load.
- If one WAN interface’s connection goes down, the ISG50 sends traffic through another member of the trunk.
- For example, you connect one WAN interface to one ISP and connect a second WAN interface to a second ISP. The ISG50 balances the WAN traffic load between the connections. If one interface's connection goes down, the ISG50 can automatically send its traffic through another interface.

You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

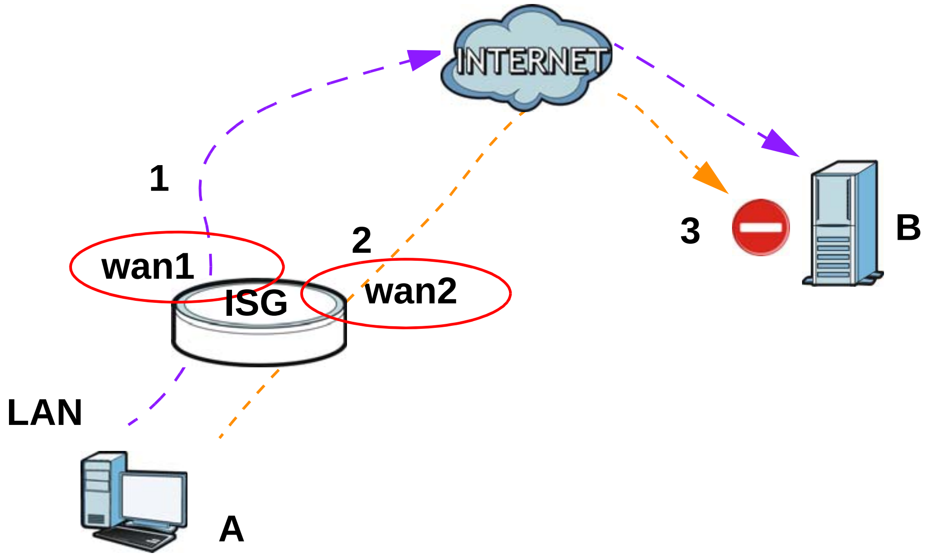
- If that interface’s connection goes down, the ISG50 can still send its traffic through another interface.

- You can define multiple trunks for the same physical interfaces.

Link Sticking

You can have the ISG50 send each local computer's traffic that is going to the same destination through a single WAN interface for a specified period of time. This is useful when a server requires authentication. For example, the ISG50 sends a user's traffic through one WAN IP address when he logs into a server B. If the user's subsequent sessions came from a different WAN IP address, the server would deny them. Here is an example.

Figure 188 Link Sticking



1 LAN user **A** logs into server **B** on the Internet. The ISG50 uses wan1 to send the request to server **B**.

2 The ISG50 is using active/active load balancing. So when LAN user **A** tries to access something on the server, the request goes out through wan2.

3 The server finds that the request comes from wan2's IP address instead of wan1's IP address and rejects the request.

If link sticking had been configured, the ISG50 would have still used wan1 to send LAN user **A**'s request to the server and server would have given the user **A** access.

Load Balancing Algorithms

The following sections describe the load balancing algorithms the ISG50 can use to decide which interface the traffic (from the LAN) should use for a session[2]. The available bandwidth you configure on the ISG50 refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

---

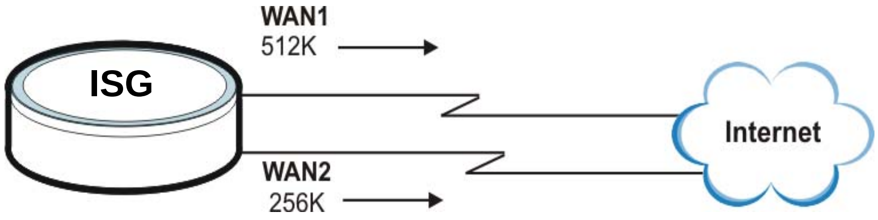
[2] In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic.

Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

Here the ISG50 has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

Figure 189 Least Load First Example



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The ISG50 calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the ISG50 will send the subsequent new session traffic through WAN 2.

Table 83 Least Load First Example

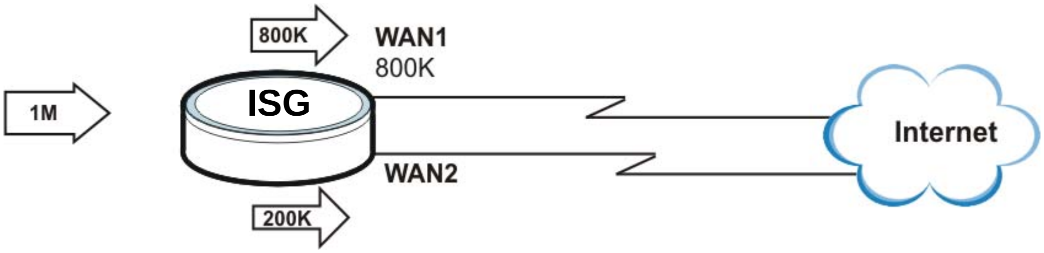
INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

Weighted Round Robin

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm (see Section 13.4 on page 288), the The Weighted Round Robin (WRR) algorithm sets the ISG50 to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more of the traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the ISG50 to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The ISG50 assigns the traffic of two sessions to wan1 for every session's traffic assigned to wan2.

Figure 190 Weighted Round Robin Algorithm Example



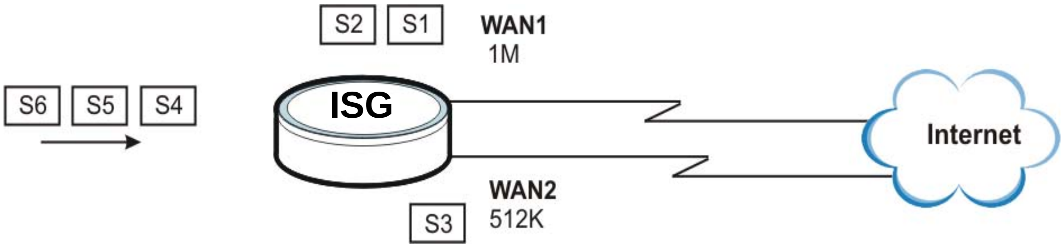
Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface’s maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

In this example figure, the upper threshold of the first interface is set to 800K. The ISG50 sends network traffic of new sessions that exceed this limit to the secondary WAN interface.

Figure 191 Spillover Algorithm Example



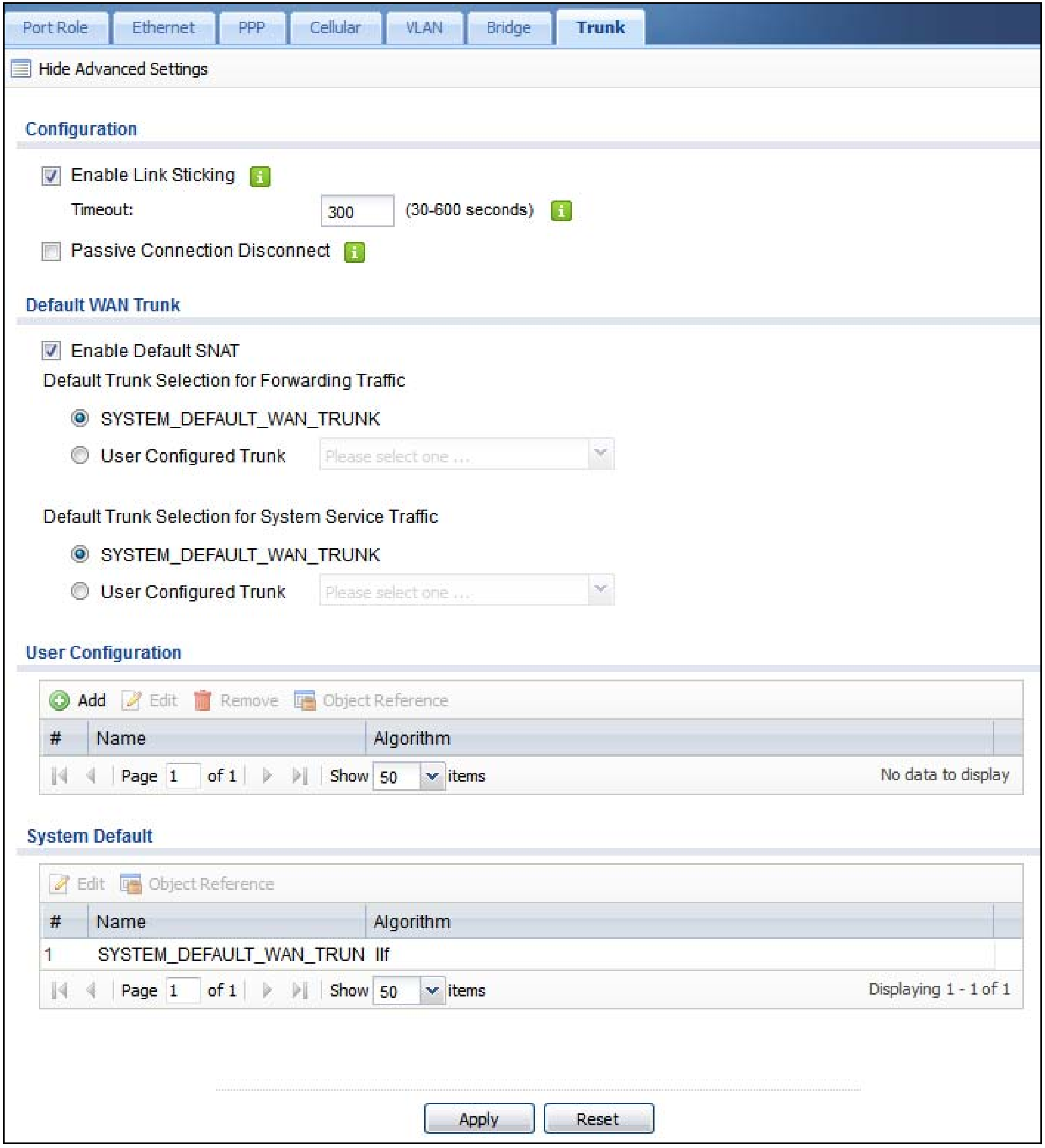
Finding Out More

- See Section 6.6.4 on page 98 for related information on the **Trunk** screens.
- See Section 7.3 on page 111 for an example of how to configure load balancing.
- See Section 13.4 on page 288 for more background information on trunks.

13.2 The Trunk Summary Screen

Click **Configuration > Network > Interface > Trunk** to open the **Trunk** screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 192 Configuration > Network > Interface > Trunk



Port Role
Ethernet
PPP
Cellular
VLAN
Bridge
Trunk
Hide Advanced Settings

Configuration

☑ Enable Link Sticking

Timeout: 300 (30-600 seconds)

☐ Passive Connection Disconnect

Default WAN Trunk

☑ Enable Default SNAT

Default Trunk Selection for Forwarding Traffic

● SYSTEM_DEFAULT_WAN_TRUNK

○ User Configured Trunk Please select one ...

Default Trunk Selection for System Service Traffic

● SYSTEM_DEFAULT_WAN_TRUNK

○ User Configured Trunk Please select one ...

User Configuration

Add
Edit
Remove
Object Reference

#	Name	Algorithm

Page 1 of 1 Show 50 items No data to display

System Default

Edit
Object Reference

#	Name	Algorithm
1	SYSTEM_DEFAULT_WAN_TRUN	llf

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Apply
Reset

The following table describes the items in this screen.

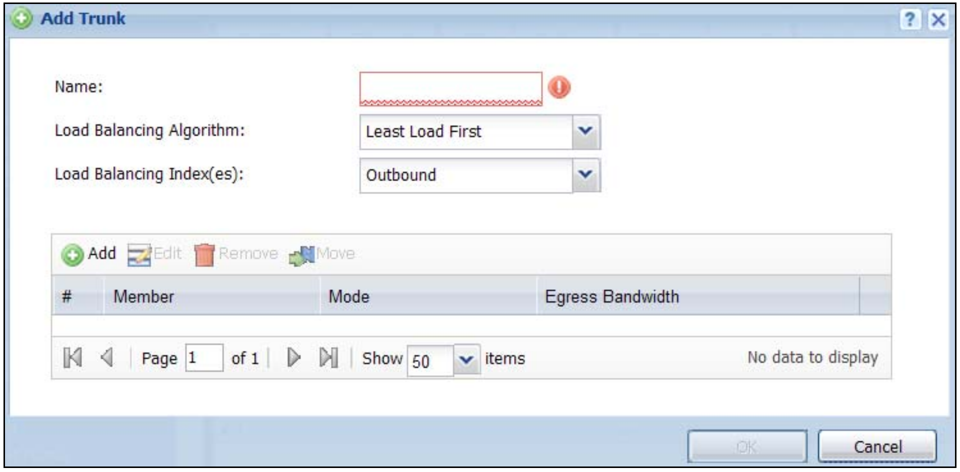
Table 84 Configuration > Network > Interface > Trunk

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
Enable Link Sticking	Enable link sticking to have the system route sessions from one source to the same destination through the same link for a period of time. This is useful for accessing server that are incompatible with a user's sessions coming from different links. For example, this is useful when a server requires authentication. This setting applies when you use load balancing and have multiple WAN interfaces set to active mode.
Timeout	Specify the time period during which sessions from one source to the same destination are to use the same link.
Passive Connection Disconnect	Select this to drop a passive mode interface’s connections when the trunk’s active mode interface comes back up.
Enable Default SNAT	Select this to have the ISG50 use the IP address of the outgoing interface as the source IP address of the packets it sends out through its WAN trunks. The ISG50 automatically adds SNAT settings for traffic it routes from internal interfaces to external interfaces.
Default Trunk Selection for Forwarding Traffic	Select the WAN trunk the ISG50 uses for routing traffic going through the ISG50.
Default Trunk Selection for System Service Traffic	Select the WAN trunk the ISG50 uses for routing traffic originating from the ISG50 itself. This includes the PBX traffic. The trunk can only have one member interface set to active mode.
User Configuration	You can create your own **User Configuration** trunks.
System Default	The ISG50 automatically adds all external interfaces into the pre-configured system default **SYSTEM_DEFAULT_WAN_TRUNK**. You cannot delete it.
Add	Click this to create a new user-configured trunk.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove a user-configured trunk, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click this button to save your changes to the ISG50.
Reset	Click this button to return the screen to its last-saved settings.

13.3 Configuring a Trunk

Click **Configuration > Network > Interface > Trunk** and then the **Add** (or **Edit**) icon to open the **Trunk Edit** screen. Use this screen to create or edit a WAN trunk entry.

Figure 193 Configuration > Network > Interface > Trunk > Add (or Edit)



Each field is described in the table below.

Table 85 Configuration > Network > Interface > Trunk > Add (or Edit)

LABEL	DESCRIPTION
Name	This is read-only if you are editing an existing trunk. When adding a new trunk, enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. Weighted round robin is activated only when the first group member interface has more traffic than it can handle. Select **Least Load First** to send new session traffic through the least utilized trunk member. Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
Load Balancing Index(es)	This field is available if you selected to use the **Least Load First** or **Spillover** method. Select **Outbound**, **Inbound**, or **Outbound + Inbound** to set the traffic to which the ISG50 applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click **Add** to add a new member interface after the selected member interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a member interface, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.

Table 85 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

LABEL	DESCRIPTION
Move	To move an interface to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this icon to open a screen where you can select an interface to be a group member.
Mode	Select **Active** to have the ISG50 always attempt to use this connection. Select **Passive** to have the ISG50 only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the ISG50 sends through each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more traffic the ISG50 sends through that interface.
Ingress Bandwidth	This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the ISG50 is to allow to come in through the interface per second.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm.It displays the maximum number of kilobits of data the ISG50 is to send out through the interface per second.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the ISG50 sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The ISG50 uses the group member interfaces in the order that they are listed.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

13.4 Trunk Technical Reference

Round Robin Load Balancing Algorithm

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

14

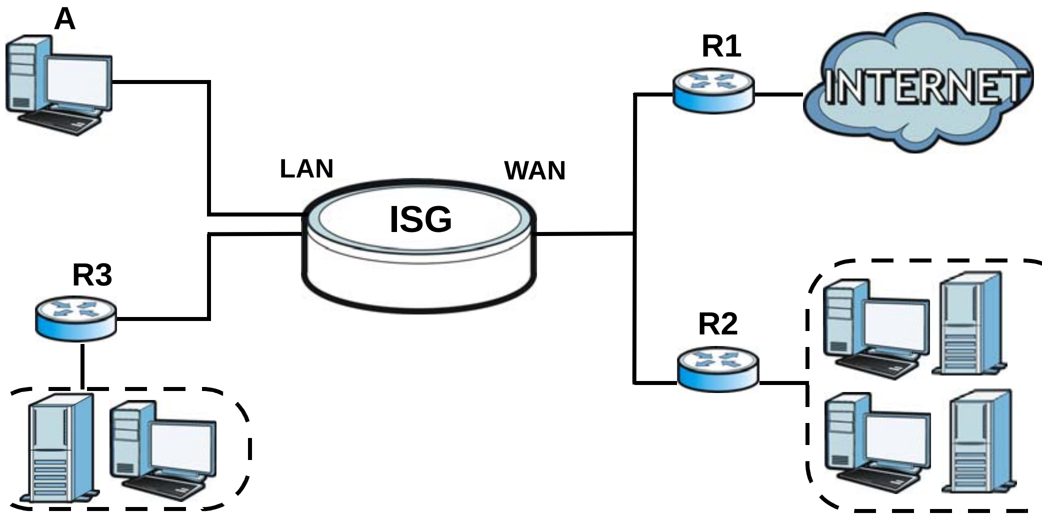
Policy and Static Routes

14.1 Policy and Static Routes Overview

Use policy routes and static routes to override the ISG50's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

For example, the next figure shows a computer (**A**) connected to the ISG50's LAN interface. The ISG50 routes most traffic from **A** to the Internet through the ISG50's default gateway (**R1**). You create one policy route to connect to services offered by your ISP behind router **R2**. You create another policy route to communicate with a separate network behind another router (**R3**) connected to the LAN.

Figure 194 Example of Policy Routing Topology



Note: You can generally just use policy routes. You only need to use static routes if you have a large network with multiple routers where you use RIP or OSPF to propagate routing information to other routers.

14.1.1 What You Can Do in this Chapter

- Use the **Policy Route** screens (see Section 14.2 on page 291) to list and configure policy routes.
- Use the **Static Route** screens (see Section 14.3 on page 297) to list and configure static routes.

14.1.2 What You Need to Know

Policy Routing

Traditionally, routing is based on the destination address only and the ISG50 takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – You can allocate bandwidth to traffic that matches routing policies and prioritize traffic. You can also use policy routes to manage other types of traffic (like ICMP traffic) and send traffic through VPN tunnels.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ISG50 performs NAT by default for traffic going to or from the **WAN** interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

Note: The ISG50 automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic.

Static Routes

The ISG50 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ISG50 send data to devices not reachable through the default gateway, use static routes. Configure static routes if you need to use RIP or OSPF to propagate the routing information to other routers. See Chapter 15 on page 302 for more on RIP and OSPF.

Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, NAT, and bandwidth management.
- Policy routes are only used within the ISG50 itself. Static routes can be propagated to other routers using RIP or OSPF.
- Policy routes take priority over static routes. If you need to use a routing policy on the ISG50 and propagate it to other routers, you could configure a policy route and an equivalent static route.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP Marking and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP (6 bits)	Unused (2 bits)

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

Finding Out More

- See Section 6.6.5 on page 98 for related information on the policy route screens.
- See Section 7.11 on page 132 for an example of creating a policy route for using multiple static public WAN IP addresses for LAN to WAN traffic.
- See Section 14.4 on page 299 for more background information on policy routing.

14.2 Policy Route Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

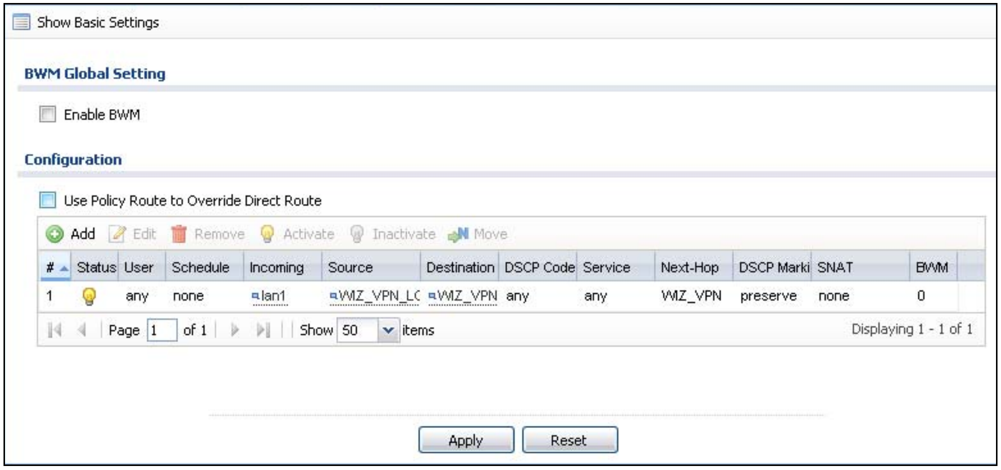
The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

Note: Policy routes do not apply to the routing of PBX traffic.

Figure 195 Configuration > Network > Routing > Policy Route



☐ Enable BWM

☐ Use Policy Route to Override Direct Route

#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marki	SNAT	BWM
1	💡	any	none	lan1	WIZ_VPN_LC	WIZ_VPN	any	any	WIZ_VPN	preserve	none	0

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 86 Configuration > Network > Routing > Policy Route

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
Enable BWM	This is a global setting for enabling or disabling bandwidth management on the ISG50. You must enable this setting to have individual policy routes.
Use Policy Route to Override Direct Route	Select this to have the ISG50 forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network. See Section 6.5.1 on page 95 for how this option affects the routing table.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This is the number of an individual policy route.
Status	This icon is lit when the entry is active, red when the next hop's connection is down, and dimmed when the entry is inactive.
User	This is the name of the user (group) object from which the packets are sent. **any** means all users.
Schedule	This is the name of the schedule object. **none** means the route is active at all times if enabled.

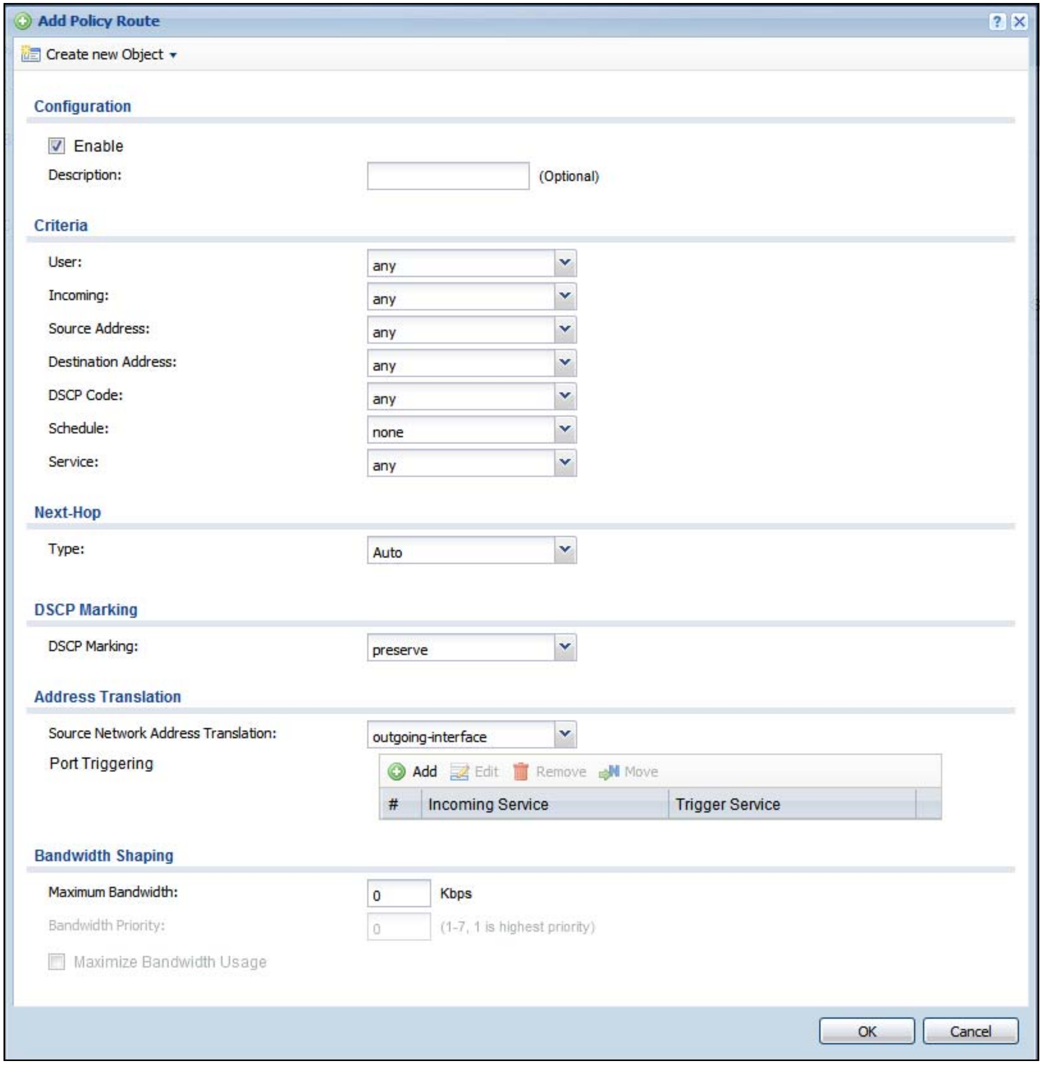
Table 86 Configuration > Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
Incoming	This is the interface on which the packets are received.
Source	This is the name of the source IP address (group) object. **any** means all IP addresses.
Destination	This is the name of the destination IP address (group) object. **any** means all IP addresses.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. **any** means all DSCP values or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The “**af**” entries stand for Assured Forwarding. The number following the “**af**” identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 299 for more details.
Service	This is the name of the service object. **any** means all services.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
DSCP Marking	This is how the ISG50 handles the DSCP value of the outgoing packets that match this route. If this field displays a DSCP value, the ISG50 applies that DSCP value to the route’s outgoing packets. **preserve** means the ISG50 does not modify the DSCP value of the route’s outgoing packets. **default** means the ISG50 sets the DSCP value of the route’s outgoing packets to 0. The “**af**” choices stand for Assured Forwarding. The number following the “**af**” identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 299 for more details.
SNAT	This is the source IP address that the route uses. It displays **none** if the ISG50 does not perform NAT for this route.
BWM	This is the maximum bandwidth allotted to the policy. **0** means there is no bandwidth limitation for this route.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

14.2.1 Policy Route Edit Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Then click the **Add** or **Edit** icon to open the **Policy Route Edit** screen. Use this screen to configure or edit a policy route.

Figure 196 Configuration > Network > Routing > Policy Route > Add



Configuration

☑ Enable

Description: (Optional)

Criteria

User: any

Incoming: any

Source Address: any

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

Next-Hop

Type: Auto

DSCP Marking

DSCP Marking: preserve

Address Translation

Source Network Address Translation: outgoing-interface

Port Triggering

#	Incoming Service	Trigger Service

Bandwidth Shaping

Maximum Bandwidth: 0 Kbps

Bandwidth Priority: 0 (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

The following table describes the labels in this screen.

Table 87 Configuration > Network > Routing > Policy Route > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent.

Table 87 Configuration > Network > Routing > Policy Route > Edit (continued)

LABEL	DESCRIPTION
Incoming	Select where the packets are coming from; any, an interface, a tunnel, or the ISG50 itself. For an interface or a tunnel, you also need to select the individual interface or VPN tunnel connection.
Source Address	Select a source IP address object from which the packets are sent.
Destination Address	Select a destination IP address object to which the traffic is being sent. If the next hop is a dynamic VPN tunnel and you enable **Auto Destination Address**, the ISG50 uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select **User Defined** to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 299 for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Schedule	Select a schedule to control when the policy route is active. **none** means the route is active at all times if enabled.
Service	Select a service or service group to identify the type of traffic to which this policy route applies.
Next-Hop	
Type	Select **Auto** to have the ISG50 use the routing table to find a next-hop and forward the matched packets automatically. Select **Gateway** to route the matched packets to the next-hop router or switch you specified in the **Gateway** field. You have to set up the next-hop router or switch as a HOST address object first. Select **VPN Tunnel** to route the matched packets via the specified VPN tunnel. Select **Trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select **Interface** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select **Gateway** in the **Type** field. Select a HOST address object. The gateway is an immediate neighbor of your ISG50 that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your ISG50's interface(s).
VPN Tunnel	This field displays when you select **VPN Tunnel** in the **Type** field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the ISG50 directly.
Auto Destination Address	This field displays when you select **VPN Tunnel** in the **Type** field. Select this to have the ISG50 use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy. Leave this cleared if you want to manually specify the destination address.
Trunk	This field displays when you select **Trunk** in the **Type** field. Select a trunk group to have the ISG50 send the packets via the interfaces in the group.

Table 87 Configuration > Network > Routing > Policy Route > Edit (continued)

LABEL	DESCRIPTION
Interface	This field displays when you select **Interface** in the **Type** field. Select an interface to have the ISG50 send traffic that matches the policy route through the specified interface.
Auto-Disable	This field displays when you select **Interface** or **Trunk** in the **Type** field. Select this to have the ISG50 automatically disable this policy route when the next hop's connection is down.
DSCP Marking	
DSCP Marking	Set how the ISG50 handles the DSCP value of the outgoing packets that match this route. Select one of the pre-defined DSCP values to apply or select **User Defined** to specify another DSCP value. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 299 for more details. Select **preserve** to have the ISG50 keep the packets' original DSCP value. Select **default** to have the ISG50 set the DSCP value of the packets to 0.
User-Defined DSCP Code	Use this field to specify a custom DSCP value.
Address Translation	Use this section to configure NAT for the policy route. This section does not apply to policy routes that use a VPN tunnel as the next hop.
Source Network Address Translation	Select **none** to not use NAT for the route. Select **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. If you select **outgoing-interface**, you can also configure port trigger settings for this interface. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets. Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route. Use **Create new Object** if you need to configure a new address (group) to use as the source IP address(es) of the packets that match this route.
Port Triggering	Configure trigger port forwarding to allow computers on the LAN to dynamically take turns using a service that uses a dedicated range of ports on the client side and a dedicated range of ports on the server side. Note: You need to create a firewall rule to allow an incoming service before using a port triggering rule.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it. You can also just double-click an entry to be able to modify it.
Remove	Select an entry and click this to delete it.
Move	The ordering of your rules is important as they are applied in order of their numbering. To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the entry.
#	This is the rule index number.

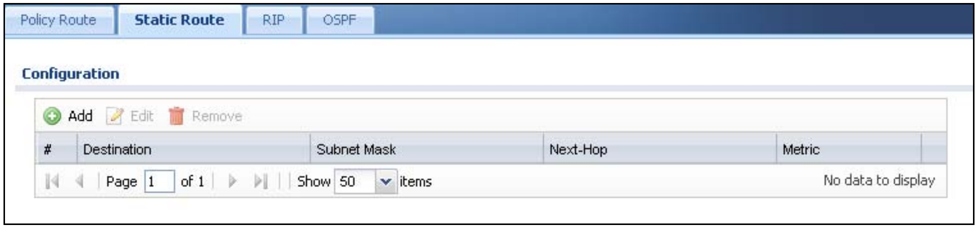
Table 87 Configuration > Network > Routing > Policy Route > Edit (continued)

LABEL	DESCRIPTION
Incoming Service	Select the service that the client computer sends to a remote server. The incoming service should have the same service or protocol type as what you configured in the **Service** field.
Trigger Service	Select a service that a remote server sends. It causes (triggers) the ISG50 to forward the traffic (received on the **outgoing interface**) to the client computer that requested the service.
Bandwidth Shaping	This allows you to allocate bandwidth to a route and prioritize traffic that matches the routing policy. You must also enable bandwidth management in the main policy route screen (**Network > Routing > Policy Route**) in order to apply bandwidth shaping.
Maximum Bandwidth	Specify the maximum bandwidth (from 1 to 1048576) allowed for the route in kbps. If you enter **0** here, there is no bandwidth limitation for the route. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth. To reserve bandwidth for traffic that does not match any of the policy routes, leave some of the interface's bandwidth unbudgeted and do not enable **Maximize Bandwidth Usage**.
Bandwidth Priority	Enter a number between 1 and 7 to set the priority for traffic. The smaller the number, the higher the priority. If you set the maximum bandwidth to **0**, the bandwidth priority will be changed to **0** after you click **OK**. That means the route has the highest priority and will get all the bandwidth it needs up to the maximum available. A route with higher priority is given bandwidth before a route with lower priority. If you set routes to have the same priority, then bandwidth is divided equally amongst those routes.
Maximize Bandwidth Usage	Select this check box to have the ISG50 divide up all of the interface's unallocated and/or unused bandwidth among the policy routes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match any of the policy routes.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

14.3 IP Static Route Screen

Click **Configuration > Network > Routing > Static Route** to open the **Static Route** screen. This screen displays the configured static routes. Configure static routes to be able to use RIP or OSPF to propagate the routing information to other routers.

Figure 197 Configuration > Network > Routing > Static Route



The following table describes the labels in this screen.

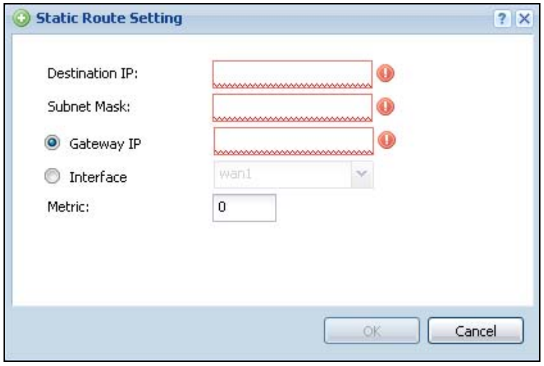
Table 88 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your ISG50's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the ISG50's routes. The smaller the number, the higher priority the route has.

14.3.1 Static Route Add/Edit Screen

Select a static route index number and click **Add** or **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 198 Configuration > Network > Routing > Static Route > Add



Destination IP:
Subnet Mask:
● Gateway IP
○ Interface wan1
Metric: 0

The following table describes the labels in this screen.

Table 89 Configuration > Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	Enter the IP subnet mask here.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ISG50's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.

Table 89 Configuration > Network > Routing > Static Route > Add (continued)

LABEL	DESCRIPTION
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

14.4 Policy Routing Technical Reference

Here is more detailed information about some of the features you can configure in policy routing.

NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 90 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set the port(s) and IP address to forward a service (coming in from the remote server) to a client computer. The problem is that port forwarding only forwards a service to a single IP address. In order to use the same service on a different computer, you have to manually replace the client computer's IP address with another client computer's IP address.

Port triggering allows the client computer to take turns using a service dynamically. Whenever a client computer’s packets match the routing policy, it can use the pre-defined port triggering setting to connect to the remote server without manually configuring a port forwarding rule for each client computer.

Port triggering is used especially when the remote server responses using a different port from the port the client computer used to request a service. The ISG50 records the IP address of a client computer that sends traffic to a remote server to request a service (incoming service). When the ISG50 receives a new connection (trigger service) from the remote server, the ISG50 forwards the traffic to the IP address of the client computer that sent the request.

In the following example, you configure two services for port triggering:

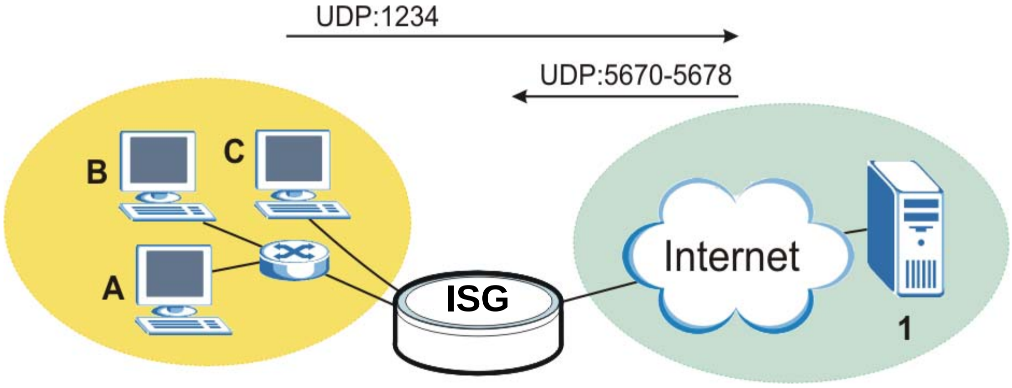
Incoming service: Game (UDP: 1234)
Trigger service: Game-1 (UDP: 5670-5678)

1 Computer **A** wants to play a multiplayer online game and tries to connect to game server **1** using port 1234. The ISG50 records the IP address of computer **A** when the packets match a policy with SNAT configured.

2 Game server **1** responds using a port number ranging between 5670 - 5678. The ISG50 allows and forwards the traffic to computer **A**.

3 Computer **A** and game server **1** are connected to each other until the connection is closed or times out. Any other computers (such as **B** or **C**) cannot connect to remote server **1** using the same port triggering rule as computer **A** unless they are using a different next hop (gateway, outgoing interface, VPN tunnel or trunk) from computer **A** or until the connection is closed or times out.

Figure 199 Trigger Port Forwarding Example



Maximize Bandwidth Usage

The maximize bandwidth usage option allows the ISG50 to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

When you enable maximize bandwidth usage, the ISG50 first makes sure that each policy route gets up to its bandwidth allotment. Next, the ISG50 divides up an interface’s available bandwidth (bandwidth that is unbudgeted or unused by the policy routes) depending on how many policy routes require more bandwidth and on their priority levels. When only one policy route requires more bandwidth, the ISG50 gives the extra bandwidth to that policy route.

When multiple policy routes require more bandwidth, the ISG50 gives the highest priority policy routes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority policy routes if there is still bandwidth available. The ISG50 distributes the available bandwidth equally among policy routes with the same priority level.

15

Routing Protocols

15.1 Routing Protocols Overview

Routing protocols give the ISG50 routing information about the network from other routers. The ISG50 stores this routing information in the routing table it uses to make routing decisions. In turn, the ISG50 can also use routing protocols to propagate routing information to other routers. See Section 6.7 on page 103 for related information on the RIP and OSPF screens.

Routing protocols are usually only used in networks using multiple routers like campuses or large enterprises.

15.1.1 What You Can Do in this Chapter

- Use the **RIP** screen (see Section 15.2 on page 302) to configure the ISG50 to use RIP to receive and/or send routing information.
- Use the **OSPF** screen (see Section 15.3 on page 304) to configure general OSPF settings and manage OSPF areas.
- Use the **OSPF Area Add/Edit** screen (see Section 15.3.2 on page 309) to create or edit an OSPF area.

15.1.2 What You Need to Know

The ISG50 supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared here and discussed further in the rest of the chapter.

Table 91 RIP vs. OSPF

	RIP	OSPF
Network Size	Small (with up to 15 routers)	Large
Metric	Hop count	Bandwidth, hop count, throughput, round trip time and reliability.
Convergence	Slow	Fast

Finding Out More

See Section 15.4 on page 311 for background information on routing protocols.

15.2 The RIP Screen

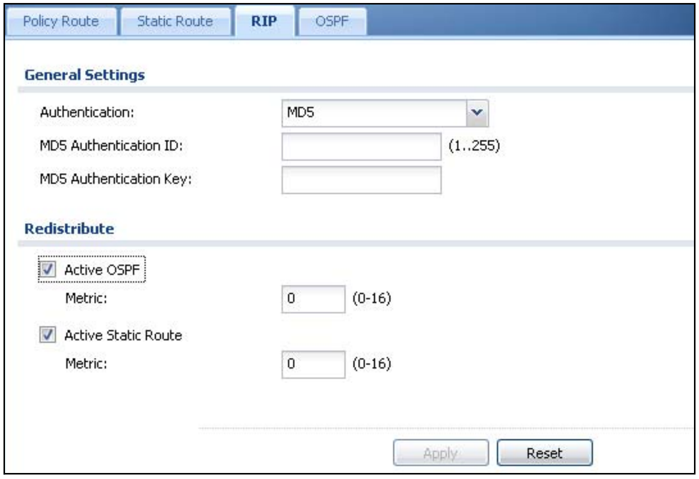
RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

- In the ISG50, you can configure two sets of RIP settings before you can use it in an interface.
- First, the **Authentication** field specifies how to verify that the routing information that is received is the same routing information that is sent. This is discussed in more detail in Authentication Types on page 312.
- Second, the ISG50 can also **redistribute** routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the **Metric** field to specify the cost in RIP terms.
- RIP uses UDP port 520.

Use the **RIP** screen to specify the authentication method and maintain the policies for redistribution.

Click **Configuration > Network** > **Routing > RIP** to open the following screen.

Figure 200 Configuration > Network > Routing > RIP



General Settings

Authentication: MD5

MD5 Authentication ID: (1..255)

MD5 Authentication Key:

Redistribute

☑ Active OSPF

Metric: 0 (0-16)

☑ Active Static Route

Metric: 0 (0-16)

The following table describes the labels in this screen.

Table 92 Configuration > Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	
Authentication	Select the authentication method used in the RIP network. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.

Table 92 Configuration > Network > Routing Protocol > RIP (continued)

LABEL	DESCRIPTION
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Redistribute	
Active OSPF	Select this to use RIP to advertise routes that were learned through OSPF.
Metric	Type the cost for routes provided by OSPF. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Active Static Route	Select this to use RIP to advertise routes that were learned through the static route configuration.
Metric	Type the cost for routes provided by the static route configuration. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Apply	Click this button to save your changes to the ISG50.
Reset	Click this button to return the screen to its last-saved settings.

15.3 The OSPF Screen

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.
- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

OSPF Areas

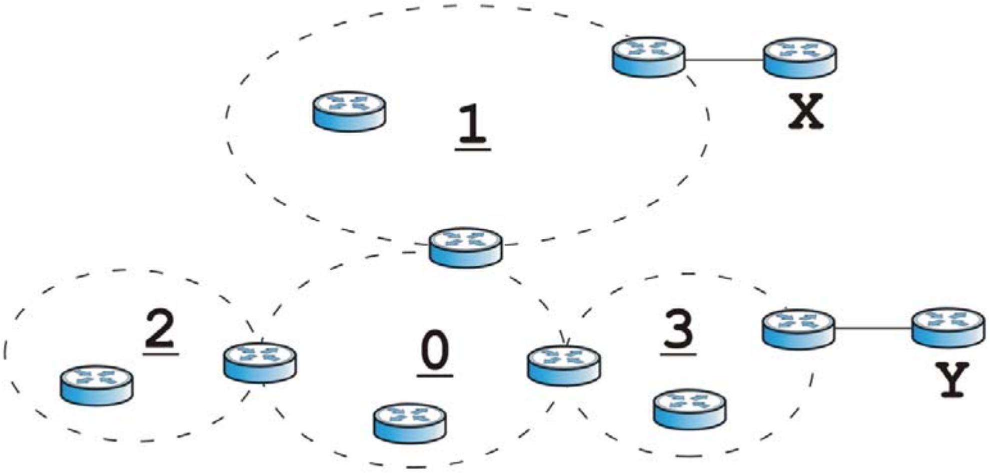
An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 201 OSPF: Types of Areas



This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.

- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.
- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

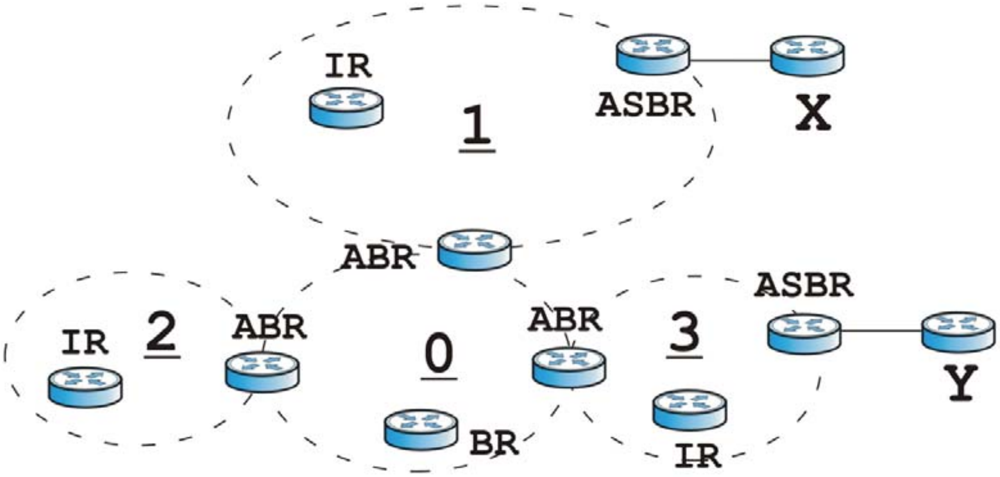
Table 93 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	No

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 202 OSPF: Types of Routers



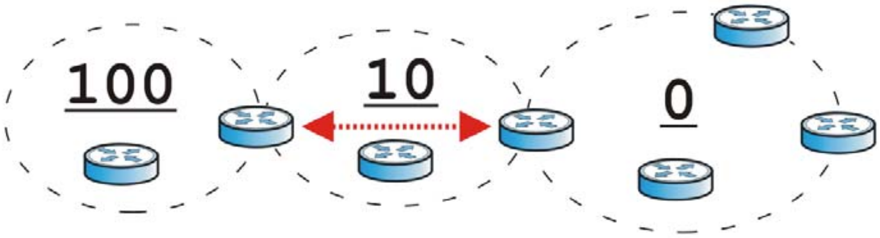
In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 203 OSPF: Virtual Link



In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

OSPF Configuration

Follow these steps when you configure OSPF on the ISG50.

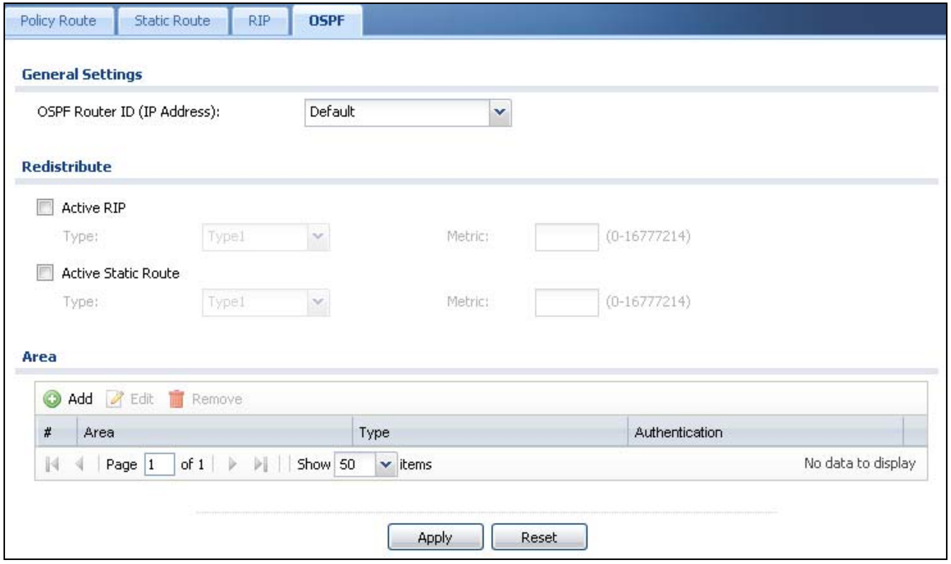
1. Enable OSPF.
2. Set up the OSPF areas.
3. Configure the appropriate interfaces. See Section 12.3.1 on page 238.
4. Set up virtual links, as needed.

15.3.1 Configuring the OSPF Screen

Use the first OSPF screen to specify the OSPF router the ISG50 uses in the OSPF AS and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the **OSPF Add/Edit** screen to add or edit them.

Click **Configuration > Network** > **Routing > OSPF** to open the following screen.

Figure 204 Configuration > Network > Routing > OSPF



OSPF Router ID (IP Address): Default

☐ Active RIP

Type: Type1 Metric: (0-16777214)

☐ Active Static Route

Type: Type1 Metric: (0-16777214)

Page 1 of 1 | Show 50 items No data to display

The following table describes the labels in this screen. See Section 15.3.2 on page 309 for more information as well.

Table 94 Configuration > Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the ISG50 uses in the OSPF AS. **Default** - the highest available IP address assigned to the interfaces is the ISG50's ID. **User Defined** - enter the ID (in IP address format) in the field that appears when you select **User Defined**.
Redistribute	
Active RIP	Select this to advertise routes that were learned from RIP. The ISG50 advertises routes learned from RIP to **Normal** and **NSSA** areas but not to **Stub** areas.
Type	Select how OSPF calculates the cost associated with routing information from RIP. Choices are: **Type 1** and **Type 2**. **Type 1** - cost = OSPF AS cost + external cost (**Metric**) **Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by RIP. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Active Static Route	Select this to advertise routes that were learned from static routes. The ISG50 advertises routes learned from static routes to all types of areas.
Type	Select how OSPF calculates the cost associated with routing information from static routes. Choices are: **Type 1** and **Type 2**. **Type 1** - cost = OSPF AS cost + external cost (**Metric**) **Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored.

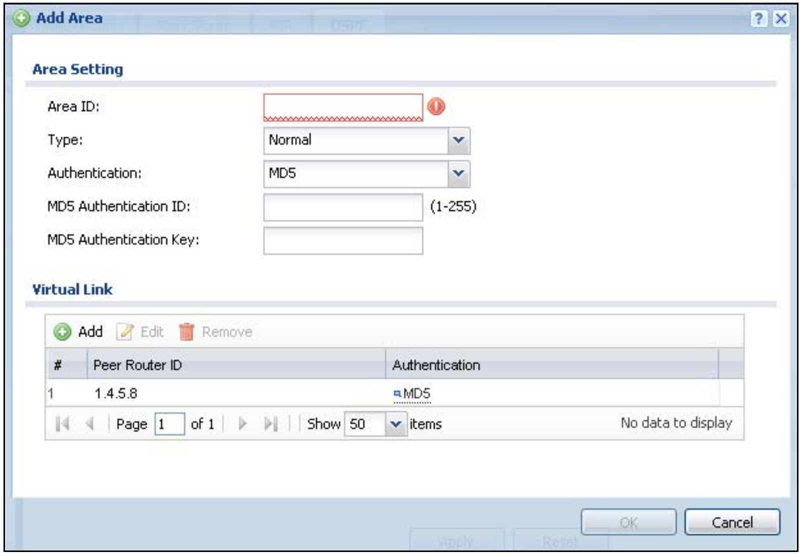
Table 94 Configuration > Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Metric	Type the external cost for routes provided by static routes. The metric represents the “cost” of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Area	This section displays information about OSPF areas in the ISG50.
Add	Click this to create a new OSPF area.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the **Type** field above.
Authentication	This field displays the default authentication method in the area.
Apply	Click this button to save your changes to the ISG50.
Reset	Click this button to return the screen to its last-saved settings.

15.3.2 OSPF Area Add/Edit Screen

The **OSPF Area Add/Edit** screen allows you to create a new area or edit an existing one. To access this screen, go to the **OSPF** summary screen (see Section 15.3 on page 304), and click either the **Add** icon or an **Edit** icon.

Figure 205 Configuration > Network > Routing > OSPF > Add



Add Area

Area Setting

Area ID:
Type: Normal
Authentication: MD5
MD5 Authentication ID: (1-255)
MD5 Authentication Key:

Virtual Link

#	Peer Router ID	Authentication
1	1.4.5.8	MD5

Page 1 of 1 Show 50 items No data to display

The following table describes the labels in this screen.

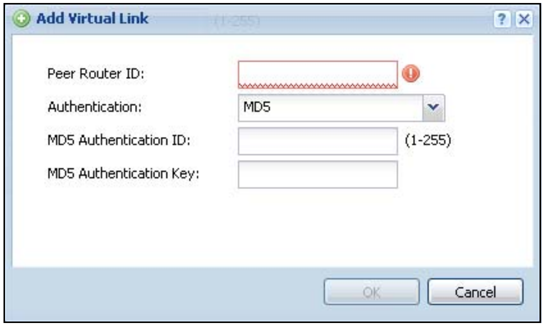
Table 95 Configuration > Network > Routing > OSPF > Add

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	Select the type of OSPF area. **Normal** - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. **Stub** - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. **NSSA** - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	Select the default authentication method used in the area. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the **Type** is **Normal**. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
Add	Click this to create a new virtual link.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	This is the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	This is the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). Hover your cursor over this label to display the password. **MD5** uses an MD5 password and authentication ID (most secure). Hover your cursor over this label to display the authentication ID and key. **Same as Area** has the virtual link also use the **Authentication** settings above.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

15.3.3 Virtual Link Add/Edit Screen

The **Virtual Link Add/Edit** screen allows you to create a new virtual link or edit an existing one. When the OSPF add or edit screen (see Section 15.3.2 on page 309) has the Type set to Normal, a Virtual Link table displays. Click either the **Add** icon or an entry and the **Edit** icon to display a screen like the following.

Figure 206 Configuration > Network > Routing > OSPF > Add > Add



Authentication: MD5

The following table describes the labels in this screen.

Table 96 Configuration > Network > Routing > OSPF > Add > Add

LABEL	DESCRIPTION
Peer Router ID	Enter the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	Select the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure). **Same as Area** has the virtual link also use the **Authentication** settings above.
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

15.4 Routing Protocol Technical Reference

Here is more detailed information about RIP and OSPF.

Authentication Types

Authentication is used to guarantee the integrity, but not the confidentiality, of routing updates. The transmitting router uses its key to encrypt the original message into a smaller message, and the smaller message is transmitted with the original message. The receiving router uses its key to encrypt the received message and then verifies that it matches the smaller message sent with it. If the received message is verified, then the receiving router accepts the updated routing information. The transmitting and receiving routers must have the same key.

The ISG50 supports three types of authentication for RIP and OSPF routing protocols:

- **None** - no authentication is used.
- **Text** – authentication using a plain text password, and the (unencrypted) password is sent over the network. This method is usually used temporarily to prevent network problems.
- **MD5** – authentication using an MD5 password and authentication ID.

MD5 is an authentication method that produces a 128-bit checksum, called a message-digest, for each packet. It also includes an authentication ID, which can be set to any value between 1 and 255. The ISG50 only accepts packets if these conditions are satisfied.

- The packet’s authentication ID is the same as the authentication ID of the interface that received it.
- The packet’s message-digest is the same as the one the ISG50 calculates using the MD5 password.

For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces. For OSPF, the ISG50 supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated **Authentication Type** field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information.

16

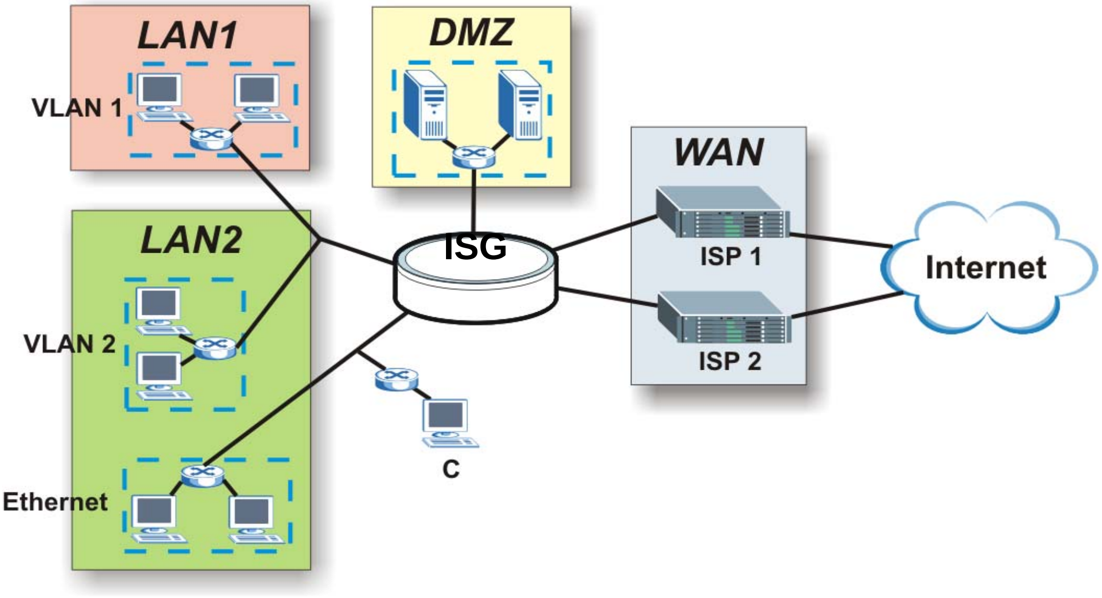
Zones

16.1 Zones Overview

Set up zones to configure network security and network policies in the ISG50. A zone is a group of interfaces and/or VPN tunnels. The ISG50 uses zones instead of interfaces in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 207 Example: Zones



16.1.1 What You Can Do in this Chapter

Use the **Zone** screens (see Section 16.2 on page 314) to manage the ISG50's zones.

16.1.2 What You Need to Know

Effects of Zones on Different Types of Traffic

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic--which are affected differently by zone-based security and policy settings.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 207 on page 313, traffic between VLAN 2 and the Ethernet is intra-zone traffic.
- In each zone, you can either allow or prohibit all intra-zone traffic. For example, in Figure 207 on page 313, you might allow intra-zone traffic in the LAN zone but prohibit it in the WAN zone.
- You can also set up firewall rules to control intra-zone traffic (for example, DMZ-to-DMZ), but many other types of zone-based security and policy settings do not affect intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 207 on page 313, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 207 on page 313, traffic to or from computer **C** is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

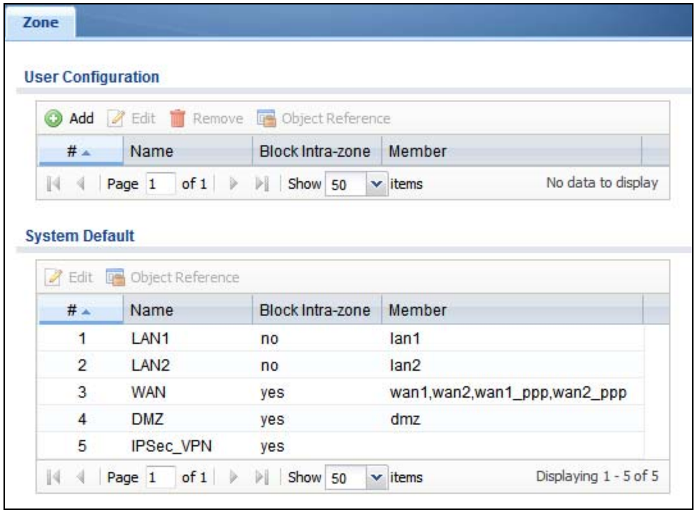
Finding Out More

- See Section 6.6.7 on page 99 for related information on these screens.
- See Section 7.1 on page 107 for an example of configuring Ethernet interfaces, port groups, and zones.

16.2 The Zone Screen

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Configuration > Network > Zone**.

Figure 208 Configuration > Network > Zone



#	Name	Block Intra-zone	Member

#	Name	Block Intra-zone	Member
1	LAN1	no	lan1
2	LAN2	no	lan2
3	WAN	yes	wan1,wan2,wan1_ppp,wan2_ppp
4	DMZ	yes	dmz
5	IPSec_VPN	yes	

The following table describes the labels in this screen.

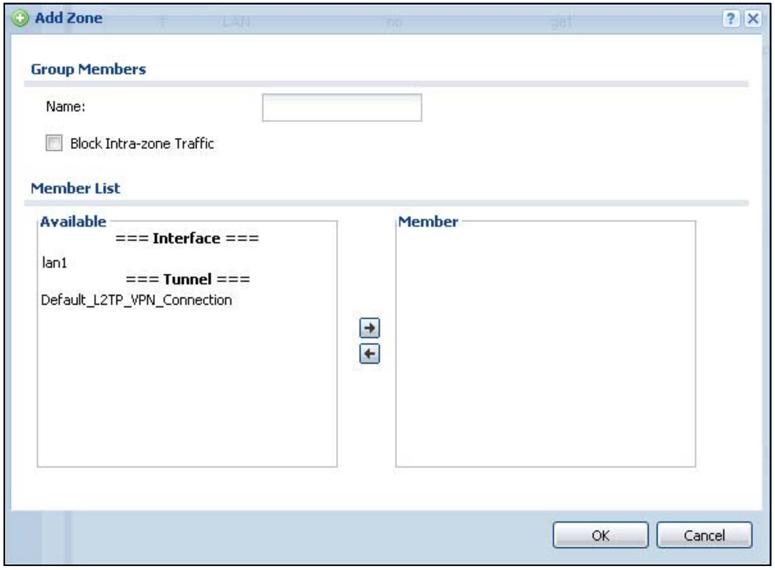
Table 97 Configuration > Network > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The ISG50 comes with pre-configured **System Default** zones that you cannot delete. You can create your own **User Configuration** zones
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the zone.
Block Intra-zone	This field indicates whether or not the ISG50 blocks network traffic between members in the zone.
Member	This field displays the names of the interfaces that belong to each zone.

16.3 Zone Edit

The **Zone Edit** screen allows you to add or edit a zone. To access this screen, go to the **Zone** screen (see Section 16.2 on page 314), and click the **Add** icon or an **Edit** icon.

Figure 209 Network > Zone > Add


Add Zone
Group Members
Name:
☐ Block Intra-zone Traffic
Member List
Available
=== Interface ===
lan1
=== Tunnel ===
Default_L2TP_VPN_Connection
Member
OK
Cancel

The following table describes the labels in this screen.

Table 98 Network > Zone > Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Block Intra-zone Traffic	Select this check box to block network traffic between members in the zone.
Member List	**Available** lists the interfaces and VPN tunnels that do not belong to any zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them. **Member** lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

17

DDNS

17.1 DDNS Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

17.1.1 What You Can Do in this Chapter

- Use the **DDNS** screen (see Section 17.2 on page 318) to view a list of the configured DDNS domain names and their details.
- Use the **DDNS Add/Edit** screen (see Section 17.2.1 on page 319) to add a domain name to the ISG50 or to edit the configuration of an existing domain name.

17.1.2 What You Need to Know

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

You must set up a dynamic DNS account with a supported DNS service provider before you can use Dynamic DNS services with the ISG50. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the ISG50 supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 99 DDNS Service Providers

PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.no-ip.com
Peanut Hull	Peanut Hull	www.oray.cn
3322	3322 Dynamic DNS, 3322 Static DNS	www.3322.org

Note: Record your DDNS account's user name, password, and domain name to use to configure the ISG50.

After, you configure the ISG50, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

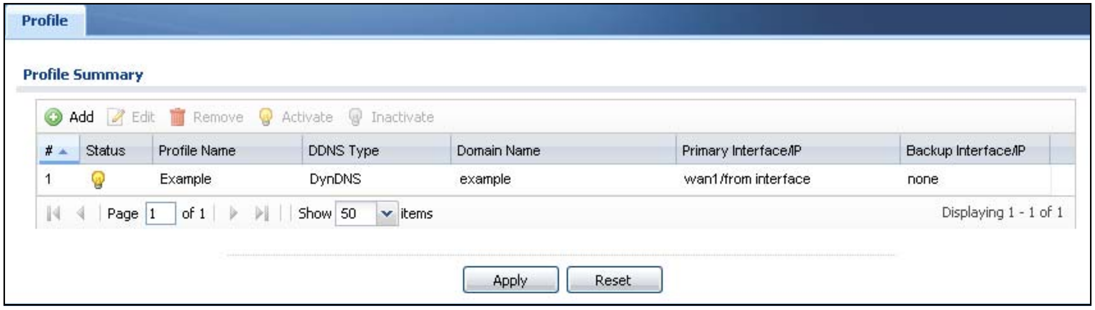
Finding Out More

See Section 6.6.8 on page 100 for related information on these screens.

17.2 The DDNS Screen

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names. Click **Configuration > Network > DDNS** to open the following screen.

Figure 210 Configuration > Network > DDNS



#	Status	Profile Name	DDNS Type	Domain Name	Primary Interface/IP	Backup Interface/IP
1	💡	Example	DynDNS	example	wan1/from interface	none

The following table describes the labels in this screen.

Table 100 Configuration > Network > DDNS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This is the number of an individual DDNS profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field displays the descriptive profile name for this entry.
DDNS Type	This field displays which DDNS service you are using.
Domain Name	This field displays each domain name the ISG50 can route.
Primary Interface/IP	This field displays the interface to use for updating the IP address mapped to the domain name followed by how the ISG50 determines the IP address for the domain name. **from interface** - The IP address comes from the specified interface. **auto detected** -The DDNS server checks the source IP address of the packets from the ISG50 for the IP address to use for the domain name. **custom** - The IP address is static.

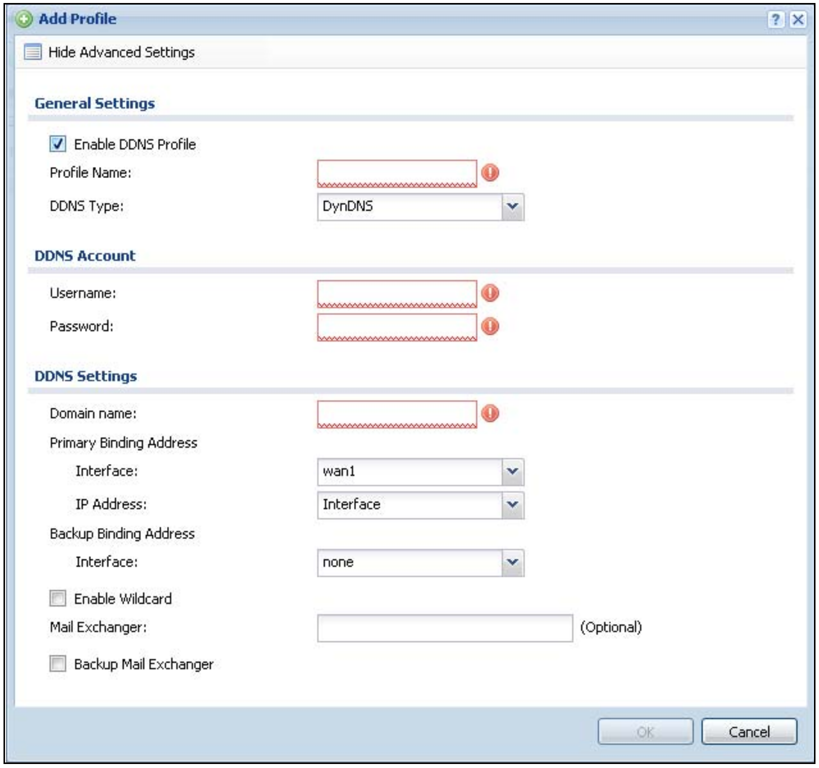
Table 100 Configuration > Network > DDNS (continued)

LABEL	DESCRIPTION
Backup Interface/IP	This field displays the alternate interface to use for updating the IP address mapped to the domain name followed by how the ISG50 determines the IP address for the domain name. The ISG50 uses the backup interface and IP address when the primary interface is disabled, its link is down or its connectivity check fails. **from interface** - The IP address comes from the specified interface. **auto detected** -The DDNS server checks the source IP address of the packets from the ISG50 for the IP address to use for the domain name. **custom** - The IP address is static.
Apply	Click this button to save your changes to the ISG50.
Reset	Click this button to return the screen to its last-saved settings.

17.2.1 The Dynamic DNS Add/Edit Screen

The **DDNS Add/Edit** screen allows you to add a domain name to the ISG50 or to edit the configuration of an existing domain name. Click **Configuration > Network > DDNS** and then an **Add** or **Edit** icon to open this screen.

Figure 211 Configuration > Network > DDNS > Add



☑ Enable DDNS Profile

Profile Name:

DDNS Type: DynDNS

Username:

Password:

Domain name:

Primary Binding Address

Interface: wan1

IP Address: Interface

Backup Binding Address

Interface: none

☐ Enable Wildcard

Mail Exchanger: (Optional)

☐ Backup Mail Exchanger

The following table describes the labels in this screen.

Table 101 Configuration > Network > DDNS > Add

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DDNS Profile	Select this check box to use this DDNS entry.
Profile Name	When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the ISG50. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is read-only when you are editing an entry.
DDNS Type	Select the type of DDNS service you are using.
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed. For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website.
Password	Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
DDNS Settings	
Domain name	Type the domain name you registered. You can use up to 255 characters.
Primary Binding Address	Use these fields to set how the ISG50 determines the IP address that is mapped to your domain name in the DDNS server. The ISG50 uses the **Backup Binding Address** if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface.
IP Address	The options available in this field vary by DDNS provider. **Interface** -The ISG50 uses the IP address of the specified interface. This option appears when you select a specific interface in the **Primary Binding Address Interface** field. **Auto** - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the ISG50 for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ISG50 and the DDNS server. Note: The ISG50 may not determine the proper IP address if there is an HTTP proxy server between the ISG50 and the DDNS server. **Custom** - If you have a static IP address, you can select this to use it for the domain name. The ISG50 still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name.
Backup Binding Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary Binding Interface** settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface. Select **None** to not use a backup address.

Table 101 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
IP Address	The options available in this field vary by DDNS provider. **Interface** -The ISG50 uses the IP address of the specified interface. This option appears when you select a specific interface in the **Backup Binding Address Interface** field. **Auto** -The DDNS server checks the source IP address of the packets from the ISG50 for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ISG50 and the DDNS server. Note: The ISG50 may not determine the proper IP address if there is an HTTP proxy server between the ISG50 and the DDNS server. **Custom** - If you have a static IP address, you can select this to use it for the domain name. The ISG50 still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name.
Enable Wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.
Mail Exchanger	This option is only available with a DynDNS account. DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise leave the field blank. See www.dyndns.org for more information about mail exchangers.
Backup Mail Exchanger	This option is only available with a DynDNS account. Select this check box if you are using DynDNS's backup service for e-mail. With this service, DynDNS holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

18

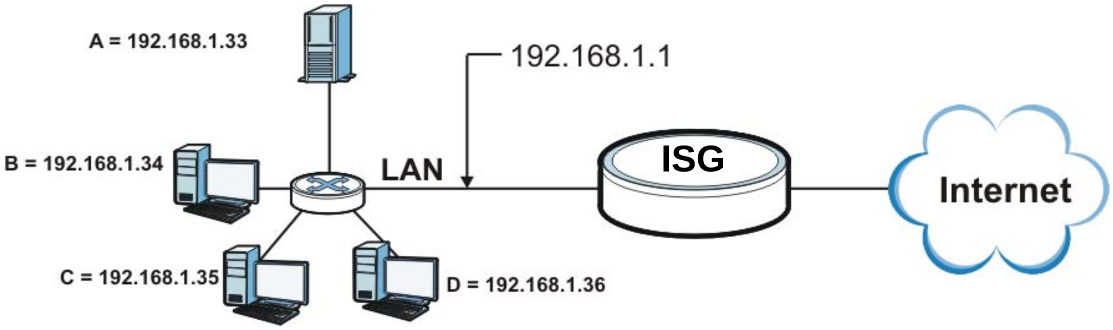
NAT

18.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network. Use Network Address Translation (NAT) to make computers on a private network behind the ISG50 available outside the private network. If the ISG50 has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 212 Multiple Servers Behind NAT Example



18.1.1 What You Can Do in this Chapter

Use the **NAT** screens (see Section 18.2 on page 324) to view and manage the list of NAT rules and see their configuration details. You can also create new NAT rules and edit or delete existing ones.

18.1.2 What You Need to Know

NAT is also known as virtual server, port forwarding, or port translation.

Finding Out More

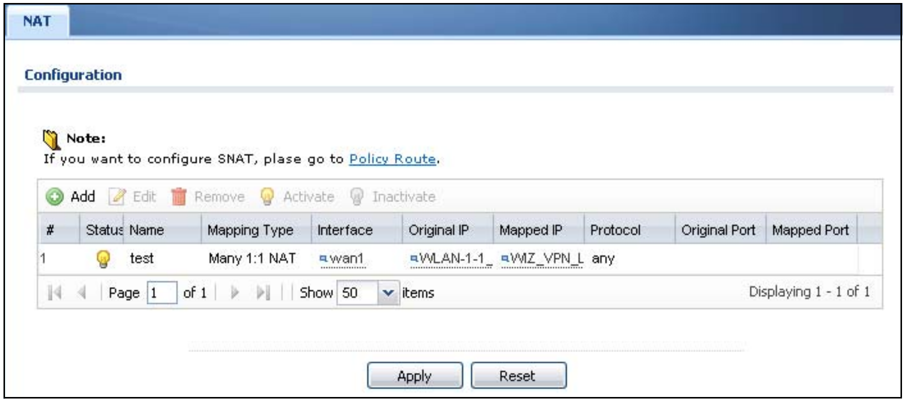
- See Section 6.6.9 on page 100 for related information on these screens.
- See Section 18.3 on page 328 for technical background information related to these screens.
- See Section 7.9.2 on page 126 for an example of how to configure NAT to allow H.323 traffic from the WAN to the LAN.

- See Section 7.10.2 on page 130 for an example of how to configure NAT to allow web traffic from the WAN to a server on the DMZ.

18.2 The NAT Screen

The **NAT** summary screen provides a summary of all NAT rules and their configuration. In addition, this screen allows you to create new NAT rules and edit and delete existing NAT rules. To access this screen, login to the Web Configurator and click **Configuration > Network > NAT**. The following screen appears, providing a summary of the existing NAT rules.

Figure 213 Configuration > Network > NAT



Note:
If you want to configure SNAT, plase go to Policy Route.

#	Status	Name	Mapping Type	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
1	💡	test	Many 1:1 NAT	wan1	WLAN-1-1_	WIZ_VPN_L	any		

The following table describes the labels in this screen.

Table 102 Configuration > Network > NAT

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the entry.
Mapping Type	This field displays what kind of NAT this entry performs: **Virtual Server**, **1:1 NAT**, or **Many 1:1 NAT**.
Interface	This field displays the interface on which packets for the NAT entry are received.
Original IP	This field displays the original destination IP address (or address object) of traffic that matches this NAT entry. It displays **any** if there is no restriction on the original destination IP address.
Mapped IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this NAT entry. It displays **any** if there is no restriction on the services.
Original Port	This field displays the original destination port(s) of packets for the NAT entry. This field is blank if there is no restriction on the original destination port.

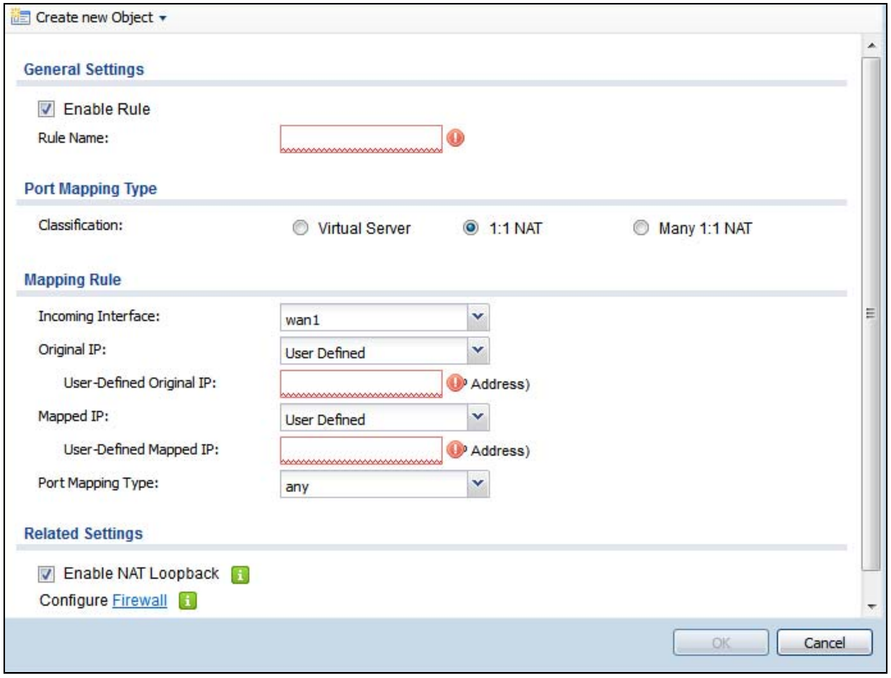
Table 102 Configuration > Network > NAT (continued)

LABEL	DESCRIPTION
Mapped Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Apply	Click this button to save your changes to the ISG50.
Reset	Click this button to return the screen to its last-saved settings.

18.2.1 The NAT Add/Edit Screen

The **NAT Add/Edit** screen lets you create new NAT rules and edit existing ones. To open this window, open the **NAT** summary screen. (See Section 18.2 on page 324.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

Figure 214 Configuration > Network > NAT > Add



☑ Enable Rule

Rule Name:

Classification: ○ Virtual Server ● 1:1 NAT ○ Many 1:1 NAT

Incoming Interface: wan1

Original IP: User Defined

User-Defined Original IP: Address)

Mapped IP: User Defined

User-Defined Mapped IP: Address)

Port Mapping Type: any

☑ Enable NAT Loopback

Configure Firewall

The following table describes the labels in this screen.

Table 103 Configuration > Network > NAT > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Use this option to turn the NAT rule on or off.
Rule Name	Type in the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 103 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Classification	Select what kind of NAT this rule is to perform. **Virtual Server** - This makes computers on a private network behind the ISG50 available to a public network outside the ISG50 (like the Internet). **1:1 NAT** - If the private network server will initiate sessions to the outside clients, select this to have the ISG50 translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server. **Many 1:1 NAT -** If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, select this to have the ISG50 translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses. One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule.
Incoming Interface	Select the interface on which packets for the NAT rule must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface.
Original IP	Specify the destination IP address of the packets received by this NAT rule's specified incoming interface. **any** - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. **User Defined** - Select this to manually enter an IP address in the **User Defined** field. For example, you could enter a static public IP assigned by the ISP without having to create a virtual interface for it. Host address - select a host address object to use the IP address it specifies. The list also includes address objects based on interface IPs. So for example you could select an address object based on a WAN interface even if it has a dynamic IP address.
User Defined Original IP	This field is available if **Original IP** is **User Defined**. Type the destination IP address that this NAT rule supports.
Original IP Subnet/Range	This field displays for Many 1:1 NAT. Select the destination IP address subnet or IP address range that this NAT rule supports. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Mapped IP	Select to which translated destination IP address this NAT rule forwards packets. **User Defined** - this NAT rule supports a specific IP address, specified in the **User Defined** field. HOST address - the drop-down box lists all the HOST address objects in the ISG50. If you select one of them, this NAT rule supports the IP address specified by the address object.
User Defined Original IP	This field is available if **Mapped IP** is **User Defined**. Type the translated destination IP address that this NAT rule supports.
Mapped IP Subnet/Range	This field displays for **Many 1:1 NAT**. Select to which translated destination IP address subnet or IP address range this NAT rule forwards packets. The original and mapped IP address subnets or ranges must have the same number of IP addresses.

Table 103 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Port Mapping Type	Use the drop-down list box to select how many original destination ports this NAT rule supports for the selected destination IP address (**Original IP**). Choices are: **any** - this NAT rule supports all the destination ports. **Service** - this NAT rule maps one service to another. **Port** - this NAT rule supports one destination port. **Ports** - this NAT rule supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service. See Appendix B on page 827 for some common port numbers.
Protocol Type	This field is available if **Mapping Type** is **Port** or **Ports**. Select the protocol (**TCP**, **UDP**, or **Any**) used by the service requesting the connection.
Original Port	This field is available if **Mapping Type** is **Port**. Enter the original destination port this NAT rule supports.
Mapped Port	This field is available if **Mapping Type** is **Port**. Enter the translated destination port if this NAT rule forwards the packet.
Original Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of original destination ports this NAT rule supports.
Original End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of original destination ports this NAT rule supports.
Mapped Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of translated destination ports if this NAT rule forwards the packet.
Mapped End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of translated destination ports if this NAT rule forwards the packet. The original port range and the mapped port range must be the same size.
Enable NAT Loopback	Enable NAT loopback to allow users connected to any interface (instead of just the specified **Incoming Interface**) to use the NAT rule's specified **Original IP** address to access the **Mapped IP** device. For users connected to the same interface as the **Mapped IP** device, the ISG50 uses that interface's IP address as the source address for the traffic it sends from the users to the **Mapped IP** device. For example, if you configure a NAT rule to forward traffic from the WAN to a LAN server, enabling NAT loopback allows users connected to other interfaces to also access the server. For LAN users, the ISG50 uses the LAN interface's IP address as the source address for the traffic it sends to the LAN server. See NAT Loopback on page 328 for more details. If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface.
Firewall	By default the firewall blocks incoming connections from external addresses. After you configure your NAT rule settings, click the **Firewall** link to configure a firewall rule to allow the NAT rule's traffic to come in. The ISG50 checks NAT rules before it applies To-ISG50 firewall rules, so To-ISG50 firewall rules do not apply to traffic that is forwarded by NAT rules. The ISG50 still checks other firewall rules according to the source IP address and mapped IP address.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to return to the **NAT** summary screen without creating the NAT rule (if it is new) or saving any changes (if it already exists).

18.3 NAT Technical Reference

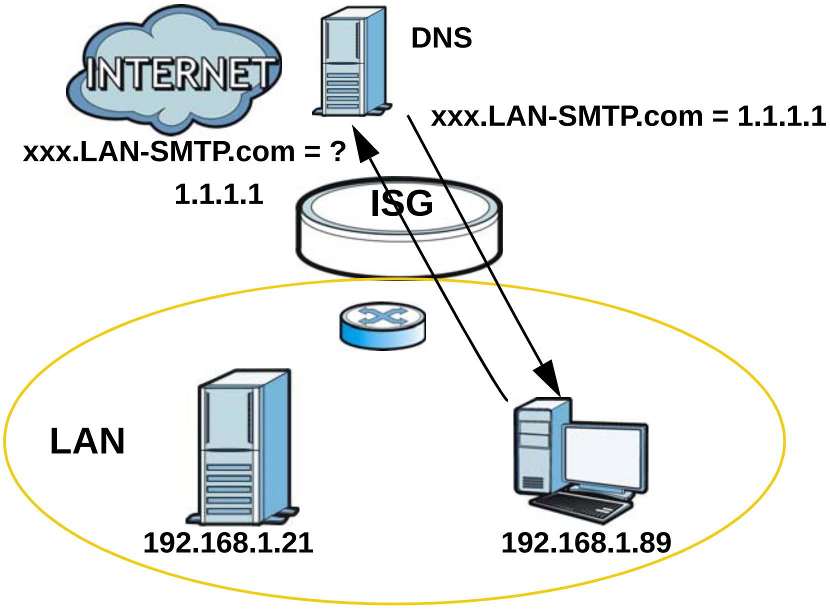
Here is more detailed information about NAT on the ISG50.

NAT Loopback

Suppose a NAT 1:1 rule maps a public IP address to the private IP address of a LAN SMTP e-mail server to give WAN users access. NAT loopback allows other users to also use the rule's original IP to access the mail server.

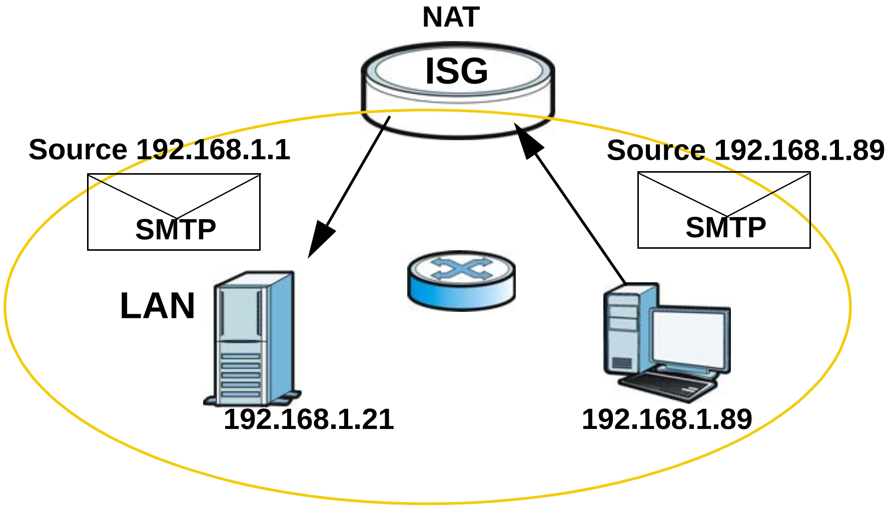
For example, a LAN user's computer at IP address 192.168.1.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 215 LAN Computer Queries a Public DNS Server


INTERNET
DNS
xxx.LAN-SMTP.com = 1.1.1.1
xxx.LAN-SMTP.com = ?
1.1.1.1
ISG
LAN
192.168.1.21
192.168.1.89

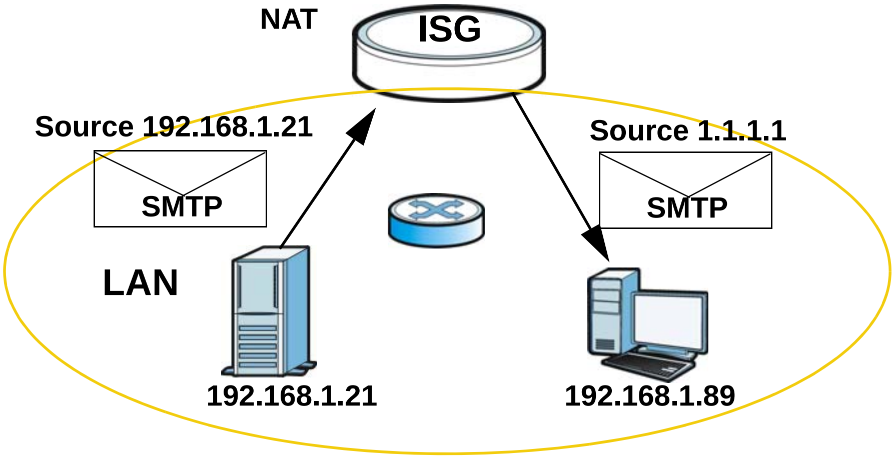
The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the ISG50's LAN interface (192.168.1.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

Figure 216 LAN to LAN Traffic


NAT
ISG
Source 192.168.1.1
SMTP
Source 192.168.1.89
SMTP
LAN
192.168.1.21
192.168.1.89

The LAN SMTP server replies to the ISG50's LAN IP address and the ISG50 changes the source address to 1.1.1.1 before sending it to the LAN user. The return traffic's source matches the original destination address (1.1.1.1). If the SMTP server replied directly to the LAN user without the traffic going through NAT, the source would not match the original destination address which would cause the LAN user's computer to shut down the session.

Figure 217 LAN to LAN Return Traffic


NAT
ISG
Source 192.168.1.21
SMTP
Source 1.1.1.1
SMTP
LAN
192.168.1.21
192.168.1.89

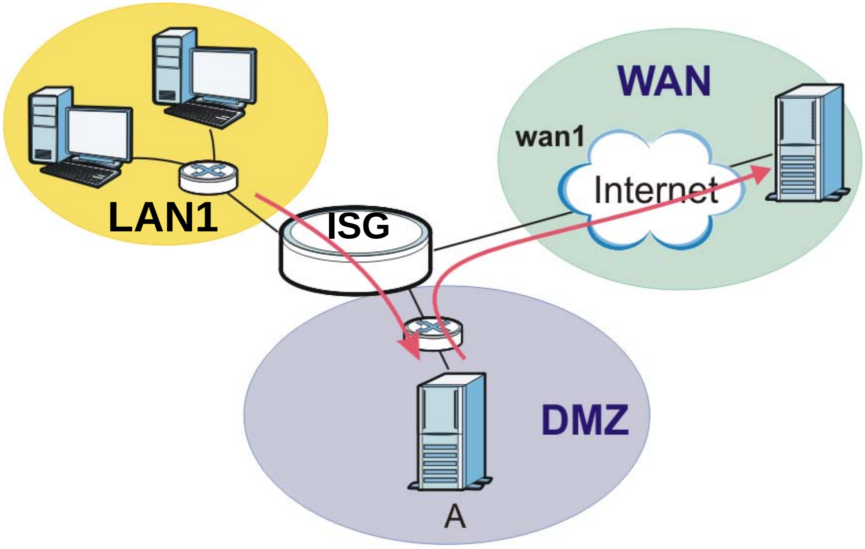
19

HTTP Redirect

19.1 Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ISG50) to a web proxy server. In the following example, proxy server **A** is connected to the **DMZ** interface. When a client connected to the **LAN1** zone wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

Figure 218 HTTP Redirect Example



19.1.1 What You Can Do in this Chapter

Use the **HTTP Redirect** screens (see Section 19.2 on page 332) to display and edit the HTTP redirect rules.

19.1.2 What You Need to Know

Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

HTTP Redirect, Firewall and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Firewall
2. HTTP Redirect
3. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the ISG50 checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no firewall rule(s) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in Figure 218 on page 331 work, make sure you have the following settings.

For HTTP traffic between **lan1** and **dmz**:

- a from LAN1 to WAN firewall rule (default) to allow HTTP requests from **lan1** to **dmz**. Responses to this request are allowed automatically.
- a HTTP redirect rule to forward HTTP traffic from **lan1** to proxy server **A**.

For HTTP traffic between **dmz** and **wan1**:

- a from DMZ to WAN firewall rule (default) to allow HTTP requests from **dmz** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

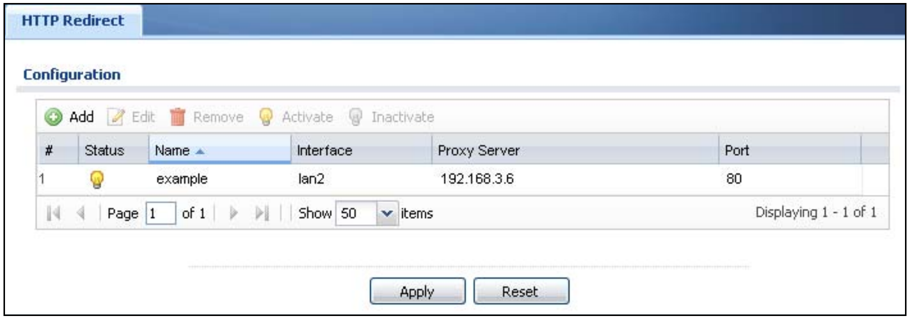
Finding Out More

See Section 6.6.10 on page 101 for related information on these screens.

19.2 The HTTP Redirect Screen

To configure redirection of a HTTP request to a proxy server, click **Configuration > Network > HTTP Redirect**. This screen displays the summary of the HTTP redirect rules.

Note: You can configure up to one HTTP redirect rule for each (incoming) interface.



#	Status	Name	Interface	Proxy Server	Port
1	●	example	lan2	192.168.3.6	80

Figure 219 Configuration > Network > HTTP Redirect

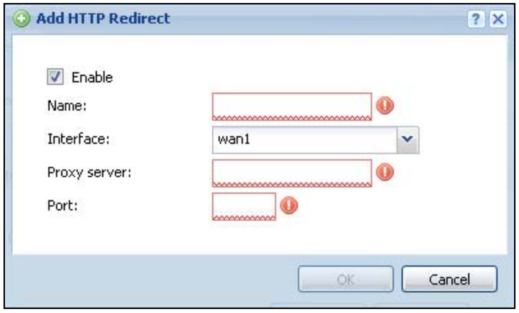
The following table describes the labels in this screen.

Table 104 Configuration > Network > HTTP Redirect

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the descriptive name of a rule.
Interface	This is the interface on which the request must be received.
Proxy Server	This is the IP address of the proxy server.
Port	This is the service port number used by the proxy server.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

19.2.1 The HTTP Redirect Edit Screen

Click **Network > HTTP Redirect** to open the **HTTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **HTTP Redirect Edit** screen where you can configure the rule.



☑ Enable

Name:

Interface: wan1

Proxy server:

Port:

Figure 220 Network > HTTP Redirect > Edit

The following table describes the labels in this screen.

Table 105 Network > HTTP Redirect > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the HTTP redirect rule on or off.
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which the HTTP request must be received for the ISG50 to forward it to the specified proxy server.
Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number that the proxy server uses.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

20

ALG

20.1 ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the ISG50's NAT.

- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.

The ALG feature is only needed for traffic that goes through the ISG50's NAT.

20.1.1 What You Can Do in this Chapter

Use the **ALG** screen (Section 20.2 on page 338) to set up H.323 and FTP ALG settings.

20.1.2 What You Need to Know

Application Layer Gateway (ALG), NAT and Firewall

The ISG50 can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as H.323) to operate properly through the ISG50's NAT and firewall. The ISG50 dynamically creates an implicit NAT session and firewall session for the application's traffic from the WAN to the LAN. The ALG on the ISG50 supports all of the ISG50's NAT mapping types.

FTP ALG

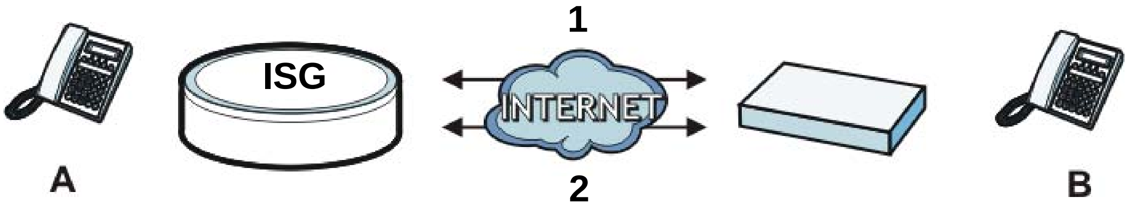
The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure NAT (port forwarding) and firewall rules if you want to allow access to the server from the WAN.

H.323 ALG

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ISG50 routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a specified port destination.
- The ISG50 allows H.323 audio connections.
- The ISG50 can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 221 H.323 ALG Example



Peer-to-Peer Calls and the ISG50

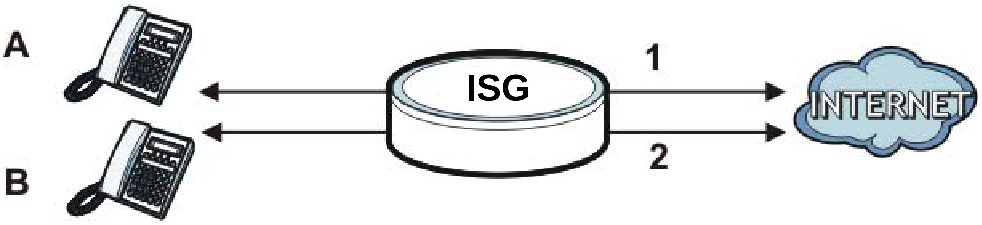
The ISG50 ALG can allow peer-to-peer VoIP calls for H.323. You must configure the firewall and NAT (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the firewall and NAT (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the ISG50 correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the firewall and NAT to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 222 VoIP Calls from the WAN with Multiple Outgoing Calls

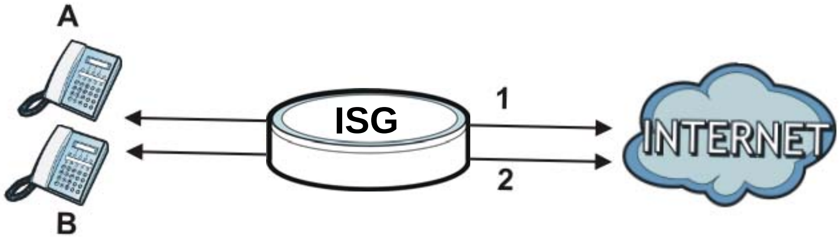


VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the ISG50, you can configure different firewall and NAT (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the ISG50 correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure firewall and NAT rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

Figure 223 VoIP with Multiple WAN IP Addresses



Finding Out More

- See Section 6.6.11 on page 101 for related information on these screens.
- See Section 7.9 on page 125 for a tutorial showing how to use the ALG for peer-to-peer H.323 traffic.
- See Section 20.3 on page 339 for ALG background/technical information.

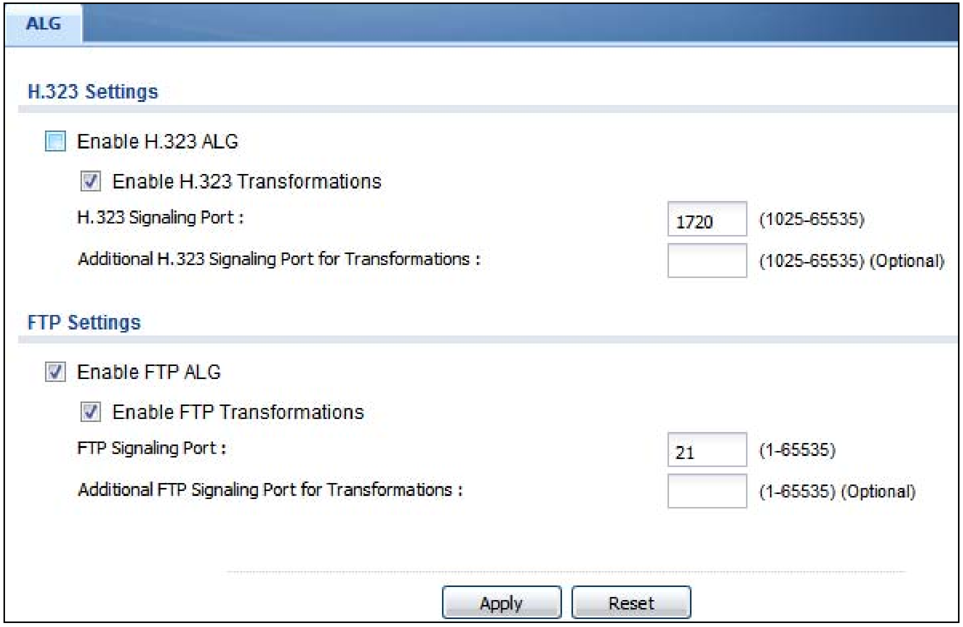
20.1.3 Before You Begin

You must also configure the firewall and enable NAT in the ISG50 to allow sessions initiated from the WAN.

20.2 The ALG Screen

Click **Configuration > Network > ALG** to open the **ALG** screen. Use this screen to turn ALGs off or on and configure the port numbers to which they apply.

Figure 224 Configuration > Network > ALG


ALG
H.323 Settings
☐ Enable H.323 ALG
☑ Enable H.323 Transformations
H.323 Signaling Port :
1720
(1025-65535)
Additional H.323 Signaling Port for Transformations :
(1025-65535) (Optional)
FTP Settings
☑ Enable FTP ALG
☑ Enable FTP Transformations
FTP Signaling Port :
21
(1-65535)
Additional FTP Signaling Port for Transformations :
(1-65535) (Optional)
Apply
Reset

The following table describes the labels in this screen.

Table 106 Configuration > Network > ALG

LABEL	DESCRIPTION
Enable H.323 ALG	Turn on the H.323 ALG to detect H.323 traffic (used for audio communications) and help build H.323 sessions through the ISG50's NAT.
Enable H.323 Transformations	Select this to have the ISG50 modify IP addresses and port numbers embedded in the H.323 data payload. You do not need to use this if you have a H.323 device or server that will modify IP addresses and port numbers embedded in the H.323 data payload.
H.323 Signaling Port	If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here.
Additional H.323 Signaling Port for Transformations	If you are also using H.323 on an additional TCP port number, enter it here.
Enable FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the ISG50's NAT.
Enable FTP Transformations	Select this option to have the ISG50 modify IP addresses and port numbers embedded in the FTP data payload to match the ISG50's NAT environment. Clear this option if you have an FTP device or server that will modify IP addresses and port numbers embedded in the FTP data payload to match the ISG50's NAT environment.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.

Table 106 Configuration > Network > ALG (continued)

LABEL	DESCRIPTION
Additional FTP Signaling Port for Transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.3 ALG Technical Reference

Here is more detailed information about the Application Layer Gateway.

ALG

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ISG50 examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ISG50 uses an application for which the ISG50 has VoIP pass through enabled, the ISG50 translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The ISG50 does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

RTP

When you make a VoIP call using H.323, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

21

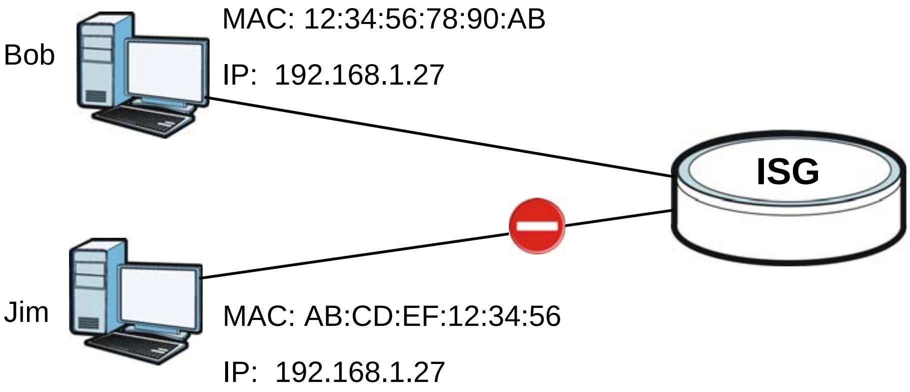
IP/MAC Binding

21.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The ISG50 uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The ISG50 then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the ISG50.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

Figure 225 IP/MAC Binding Example



21.1.1 What You Can Do in this Chapter

- Use the **Summary** and **Edit** screens (Section 21.2 on page 342) to bind IP addresses to MAC addresses.
- Use the **Exempt List** screen (Section 21.3 on page 345) to configure ranges of IP addresses to which the ISG50 does not apply IP/MAC binding.

21.1.2 What You Need to Know

DHCP

IP/MAC address bindings are based on the ISG50's dynamic and static DHCP entries.

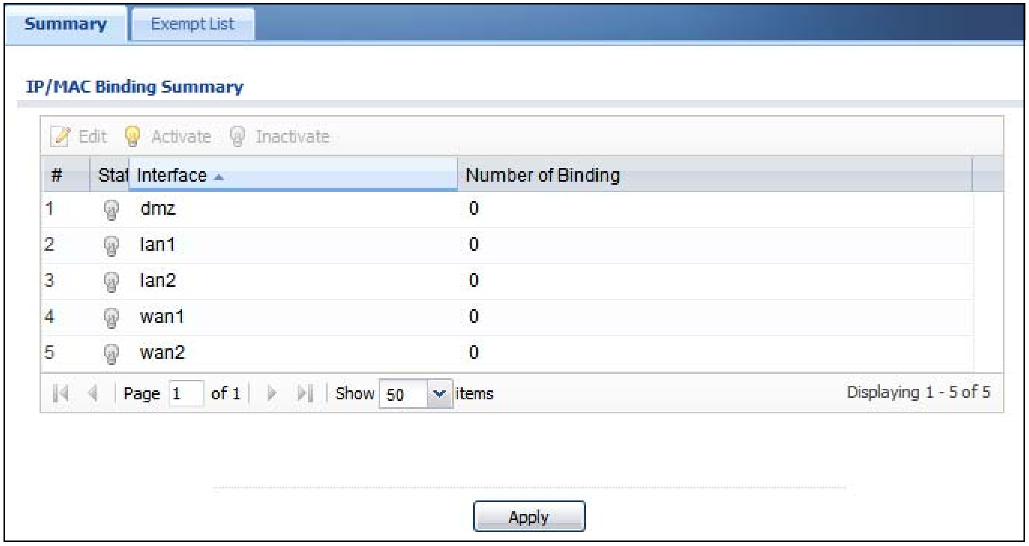
Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, and VLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

21.2 IP/MAC Binding Summary

Click **Configuration > Network > IP/MAC Binding** to open the **IP/MAC Binding Summary** screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

Figure 226 Configuration > Network > IP/MAC Binding > Summary



#	Stat	Interface	Number of Binding
1		dmz	0
2		lan1	0
3		lan2	0
4		wan1	0
5		wan2	0

The following table describes the labels in this screen.

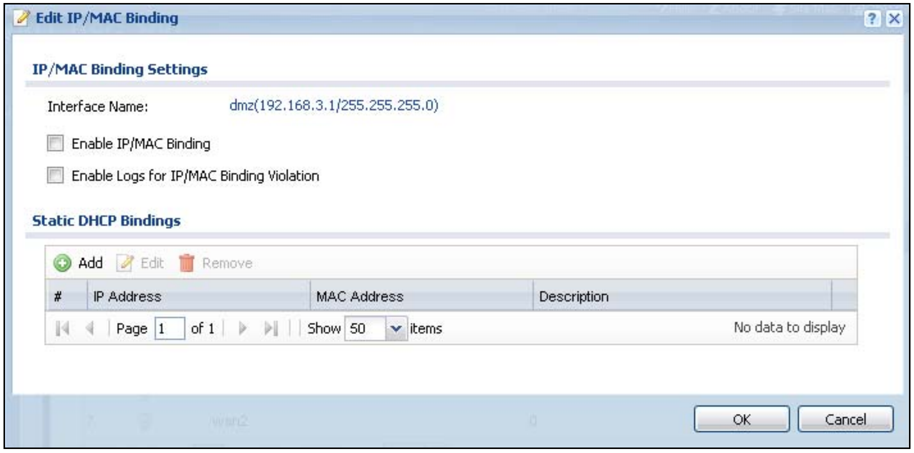
Table 107 Configuration > Network > IP/MAC Binding > Summary

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This is the name of an interface that supports IP/MAC binding.
Number of Binding	This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP.
Apply	Click **Apply** to save your changes back to the ISG50.

21.2.1 IP/MAC Binding Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 227 Configuration > Network > IP/MAC Binding > Edit



Interface Name: dmz(192.168.3.1/255.255.255.0)

☐ Enable IP/MAC Binding

☐ Enable Logs for IP/MAC Binding Violation

The following table describes the labels in this screen.

Table 108 Configuration > Network > IP/MAC Binding > Edit

LABEL	DESCRIPTION
IP/MAC Binding Settings	
Interface Name	This field displays the name of the interface within the ISG50 and the interface's IP address and subnet mask.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ISG50 generate a log if a device connected to this interface attempts to use an IP address not assigned by the ISG50.
Static DHCP Bindings	This table lists the bound IP and MAC addresses. The ISG50 checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ISG50 assigns the corresponding IP address. You can also access this table from the interface's edit screen.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This is the index number of the static DHCP entry.
IP Address	This is the IP address that the ISG50 assigns to a device with the entry's MAC address.
MAC Address	This is the MAC address of the device to which the ISG50 assigns the entry's IP address.
Description	This helps identify the entry.

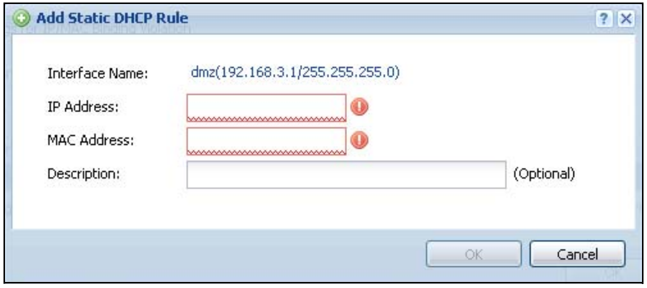
Table 108 Configuration > Network > IP/MAC Binding > Edit (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

21.2.2 Static DHCP Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Click the **Add** or **Edit** icon to open the following screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 228 Configuration > Network > IP/MAC Binding > Edit > Add



Add Static DHCP Rule

Interface Name: dmz(192.168.3.1/255.255.255.0)

IP Address:

MAC Address:

Description: (Optional)

The following table describes the labels in this screen.

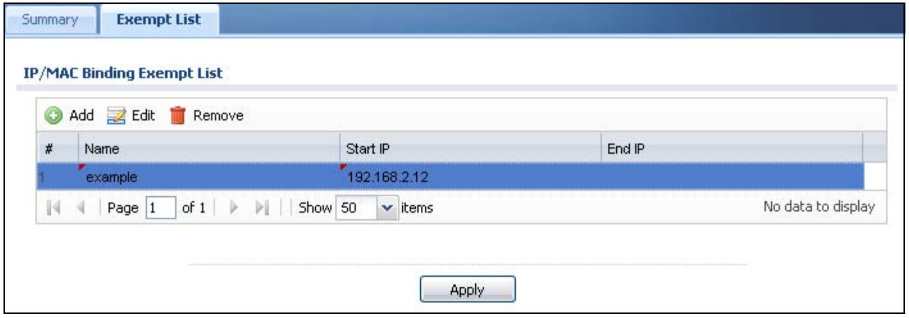
Table 109 Configuration > Network > IP/MAC Binding > Edit > Add

LABEL	DESCRIPTION
Interface Name	This field displays the name of the interface within the ISG50 and the interface's IP address and subnet mask.
IP Address	Enter the IP address that the ISG50 is to assign to a device with the entry's MAC address.
MAC Address	Enter the MAC address of the device to which the ISG50 assigns the entry's IP address.
Description	Enter up to 64 printable ASCII characters to help identify the entry. For example, you may want to list the computer's owner.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

21.3 IP/MAC Binding Exempt List

Click **Configuration > Network > IP/MAC Binding > Exempt List** to open the **IP/MAC Binding Exempt List** screen. Use this screen to configure ranges of IP addresses to which the ISG50 does not apply IP/MAC binding.

Figure 229 Configuration > Network > IP/MAC Binding > Exempt List



#	Name	Start IP	End IP
1	example	192.168.2.12	

The following table describes the labels in this screen.

Table 110 Configuration > Network > IP/MAC Binding > Exempt List

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Click an entry or select it and click **Edit** to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This is the index number of the IP/MAC binding list entry.
Name	Enter a name to help identify this entry.
Start IP	Enter the first IP address in a range of IP addresses for which the ISG50 does not apply IP/MAC binding.
End IP	Enter the last IP address in a range of IP addresses for which the ISG50 does not apply IP/MAC binding.
Apply	Click **Apply** to save your changes back to the ISG50.

22

Authentication Policy

22.1 Overview

Use authentication policies to control who can access the network. You can authenticate users (require them to log in).

22.1.1 What You Can Do in this Chapter

Use the **Configuration > Auth. Policy** screens (Section 22.2 on page 347) to create and manage authentication policies.

22.1.2 What You Need to Know

Authentication Policy and VPN

Authentication policies are applied based on a traffic flow's source and destination IP addresses. If VPN traffic matches an authentication policy's source and destination IP addresses, the user must pass authentication.

Forced User Authentication

Instead of making users for which user-aware policies have been configured go to the ISG50 **Login** screen manually, you can configure the ISG50 to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

Note: This works with HTTP traffic only. The ISG50 does display the **Login** screen when users attempt to send other kinds of traffic.

The ISG50 does not automatically route the request that prompted the login, however, so users have to make this request again.

Finding Out More

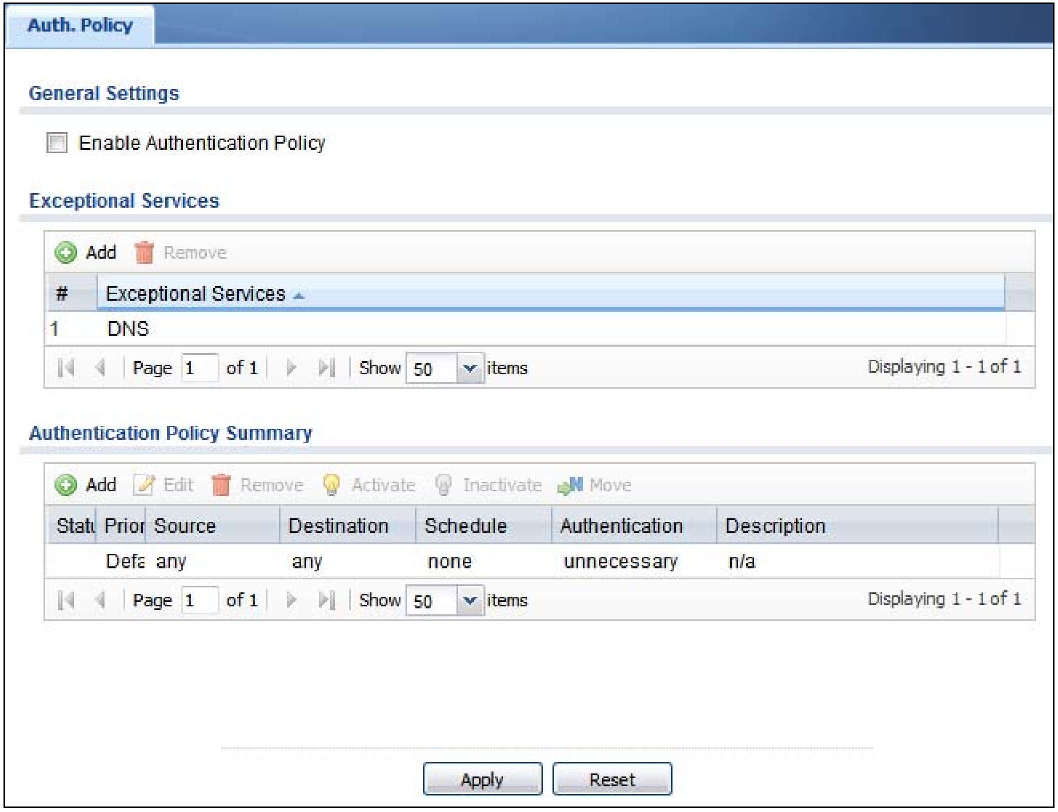
See Section 7.7 on page 122 for an example of how to use authentication policies.

22.2 Authentication Policy Screen

The **Authentication Policy** screen displays the authentication policies you have configured on the ISG50.

Click **Configuration > Auth. Policy** to display the screen.

Figure 230 Configuration > Auth. Policy


Auth. Policy
General Settings
Exceptional Services
Add
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Authentication Policy Summary
Add
Edit
Remove
Activate
Inactivate
Move
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Apply
Reset

☐ Enable Authentication Policy

#	Exceptional Services
1	DNS

Statu	Prior	Source	Destination	Schedule	Authentication	Description
	Defa	any	any	none	unnecessary	n/a

The following table gives an overview of the objects you can configure.

Table 111 Configuration > Auth. Policy

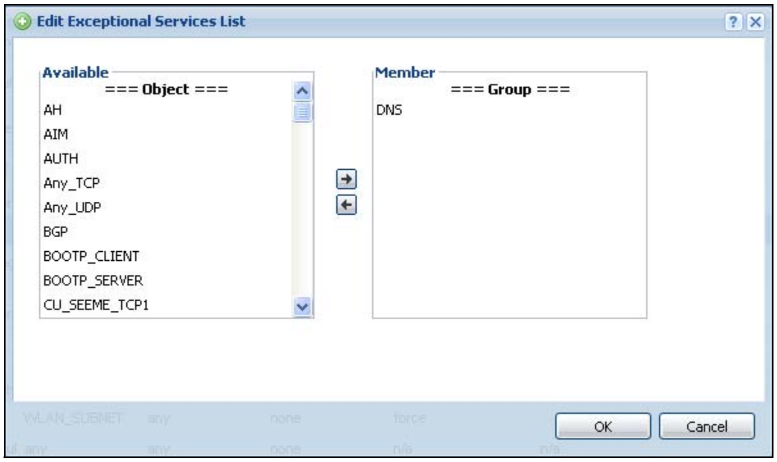
LABEL	DESCRIPTION
Enable Authentication Policy	Select this to turn on the authentication policy feature.
Exceptional Services	Use this table to list services that users can access without logging in. Click **Add** to change the list's membership. A screen appears. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button to add them. The member services are the right. Select any service that you want to remove from the member list, and click the left arrow button to remove them. Keeping DNS as a member allows users' computers to resolve domain names into IP addresses. **Figure 231** Configuration > Auth. Policy > Add Exceptional Service  Edit Exceptional Services List Available === Object === AH AIM AUTH Any_TCP Any_UDP BGP BOOTP_CLIENT BOOTP_SERVER CU_SEEME_TCP1 Member === Group === DNS OK Cancel In the table, select one or more entries and click **Remove** to delete it or them.
Authentication Policy Summary	Use this table to manage the ISG50's list of authentication policies.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of the authentication policy in the list. The priority is important as the policies are applied in order of priority. Default displays for the default authentication policy that the ISG50 uses on traffic that does not match any exceptional service or other authentication policy. You can edit the default rule but not delete it.
Source	This displays the source address object to which this policy applies.

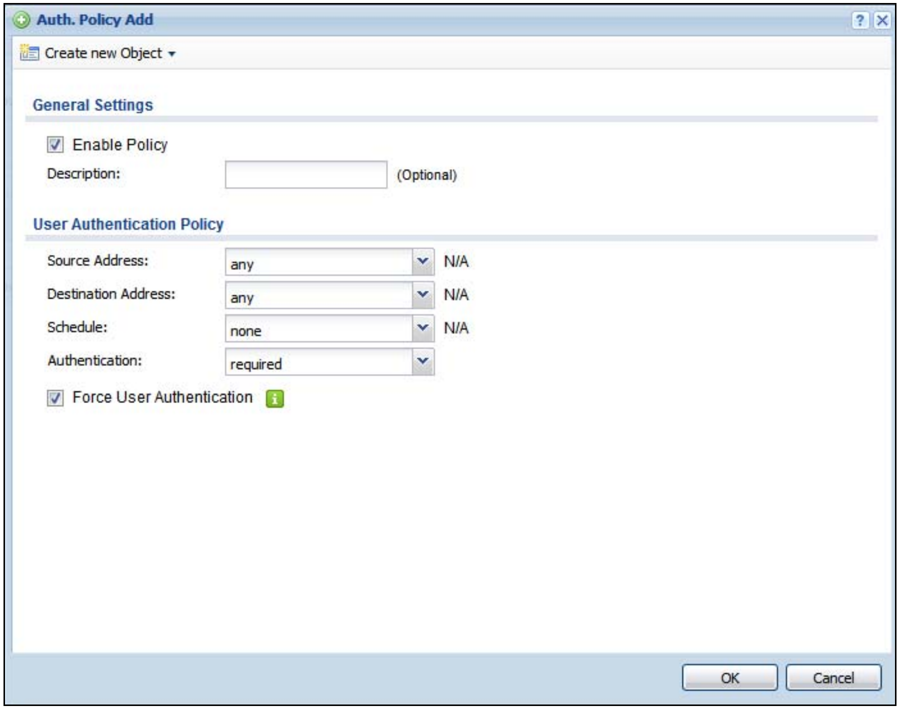
Table 111 Configuration > Auth. Policy (continued)

LABEL	DESCRIPTION
Destination	This displays the destination address object to which this policy applies.
Schedule	This field displays the schedule object that dictates when the policy applies. **none** means the policy is active at all times if enabled.
Authentication	This field displays the authentication requirement for users when their traffic matches this policy. This is **n/a** for the default policy. **unnecessary** - Users do not need to be authenticated. **required** - Users need to be authenticated. They must manually go to the login screen. The ISG50 will not redirect them to the login screen. **force** - Users need to be authenticated. The ISG50 automatically displays the login screen whenever it routes HTTP traffic for users who have not logged in yet.
Description	If the entry has a description configured, it displays here.
Apply	Click this button to save your changes to the ISG50.
Reset	Click this button to return the screen to its last-saved settings.

22.2.1 Creating/Editing an Authentication Policy

Click **Configuration > Auth. Policy** and then the **Add** (or **Edit**) icon to open the **Auth. Policy Edit** screen. Use this screen to configure an authentication policy.

Figure 232 Configuration > Auth. Policy > Add



General Settings

☑ Enable Policy

Description: (Optional)

User Authentication Policy

Source Address: any N/A

Destination Address: any N/A

Schedule: none N/A

Authentication: required

☑ Force User Authentication

The following table gives an overview of the objects you can configure.

Table 112 Configuration > Auth. Policy > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Policy	Select this check box to activate the authentication policy. This field is available for user-configured policies.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the policy. Spaces are allowed. This field is available for user-configured policies.
User Authentication Policy	Use this section of the screen to determine which traffic requires (or does not require) the senders to be authenticated in order to be routed.
Source Address	Select a source address or address group for whom this policy applies. Select **any** if the policy is effective for every source. This is **any** and not configurable for the default policy.
Destination Address	Select a destination address or address group for whom this policy applies. Select **any** if the policy is effective for every destination. This is **any** and not configurable for the default policy.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select **none** and the rule is always effective. This is **none** and not configurable for the default policy.
Authentication	Select the authentication requirement for users when their traffic matches this policy. **unnecessary** - Users do not need to be authenticated. **required** - Users need to be authenticated. They must manually go to the login screen. The ISG50 will not redirect them to the login screen.
Log	This field is available for the default policy. Select whether to have the ISG50 generate a log (**log**), log and alert (**log alert**) or not (**no**) for packets that match the default policy. See Chapter 53 on page 705 for more on logs.
Force User Authentication	This field is available for user-configured policies that require authentication. Select this to have the ISG50 automatically display the login screen when users who have not logged in yet try to send HTTP traffic.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving.

23

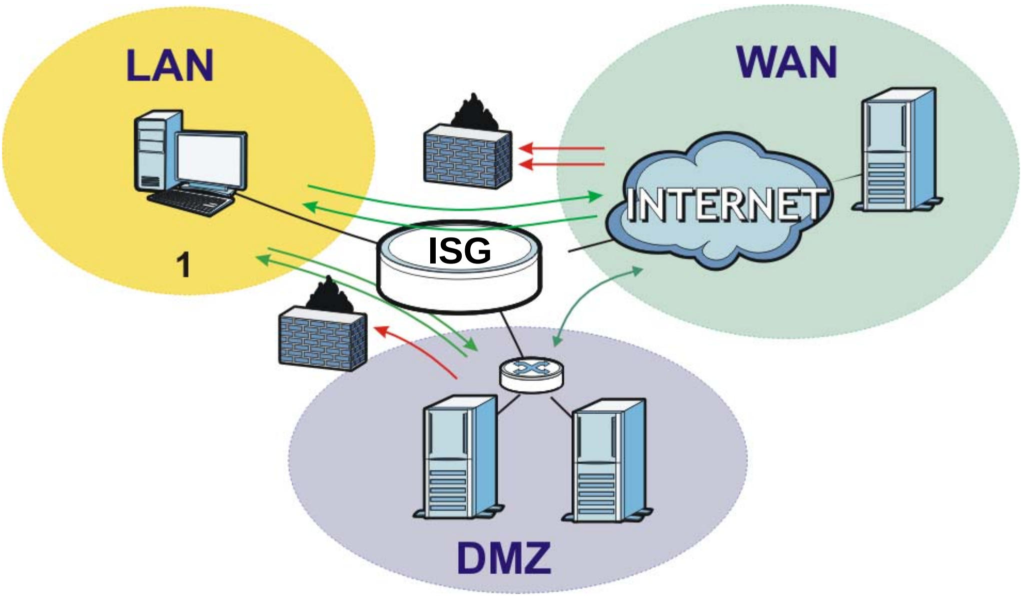
Firewall

23.1 Overview

Use the firewall to block or allow services that use static port numbers. The firewall can also limit the number of user sessions.

This figure shows the ISG50's default firewall rules in action and demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN1 zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN1 zone is blocked. Communications between the WAN and the DMZ zones are allowed. The firewall allows VPN traffic between any of the networks.

Figure 233 Default Firewall Action



23.1.1 What You Can Do in this Chapter

- Use the **Firewall** screens (Section 23.2 on page 360) to enable or disable the firewall and asymmetrical routes, and manage and configure firewall rules.
- Use the **Session Limit** screens (see Section 23.3 on page 364) to limit the number of concurrent NAT/firewall sessions a client can use.

23.1.2 What You Need to Know

Stateful Inspection

The ISG50 has a stateful inspection firewall. The ISG50 restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Zones

A zone is a group of interfaces or VPN tunnels. Group the ISG50's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

Default Firewall Behavior

Firewall rules are grouped based on the direction of travel of packets to which they apply. Here is the default firewall behavior for traffic going through the ISG50 in various directions.

Table 113 Default Firewall Behavior

FROM ZONE TO ZONE	BEHAVIOR
From WAN to Device	Traffic from the WAN to the ISG50 itself is allowed for certain default services described in To-Device Rules on page 354. All other WAN to ISG50 traffic is dropped.
From WAN to any (other than the ISG50)	Traffic from the WAN to any of the networks behind the ISG50 is dropped.
From DMZ to Device	Traffic from the DMZ to the ISG50 itself is allowed for certain default services described in To-Device Rules on page 354. All other DMZ to ISG50 traffic is dropped.
From DMZ to any (other than the ISG50)	Traffic from the DMZ to any of the networks behind the ISG50 is dropped.
From ANY to ANY	Traffic that does not match any firewall rule is allowed. So for example, LAN to WAN, LAN to DMZ traffic is allowed. This also includes traffic to or from interfaces or VPN tunnels that are not assigned to a zone (extra-zone traffic).

To-Device Rules

Rules with Device as the **To Zone** apply to traffic going to the ISG50 itself. By default:

- The firewall allows only LAN or WAN computers to access or manage the ISG50.
- The ISG50 drops most packets from the WAN zone to the ISG50 itself, except for ESP/AH/IKE/NATT/HTTPS services for VPN tunnels, and generates a log.
- The ISG50 drops most packets from the DMZ zone to the ISG50 itself, except for DNS and NetBIOS traffic, and generates a log.

When you configure a firewall rule for packets destined for the ISG50 itself, make sure it does not conflict with your service control rule. See Chapter 52 on page 665 for more information about service control (remote management). The ISG50 checks the firewall rules before the service control rules for traffic destined for the ISG50.

You can configure a To-ISG50 firewall rule (with **From Any To Device** direction) for traffic from an interface which is not in a zone.

Global Firewall Rules

Firewall rules with **from any** and/or **to any** as the packet direction are called global firewall rules. The global firewall rules are the only firewall rules that apply to an interface or VPN tunnel that is not included in a zone. The **from any** rules apply to traffic coming from the interface and the **to any** rules apply to traffic going to the interface.

Firewall Rule Criteria

The ISG50 checks the schedule, user name (user's login name on the ISG50), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ISG50 takes the action specified in the rule.

User Specific Firewall Rules

You can specify users or user groups in firewall rules. For example, to allow a specific user from any computer to access a zone by logging in to the ISG50, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ISG50 and will be disabled after the user logs out of the ISG50.

Firewall and VPN Traffic

After you create a VPN tunnel and add it to a zone, you can set the firewall rules applied to VPN traffic. If you add a VPN tunnel to an existing zone (the LAN1 zone for example), you can configure a new LAN1 to LAN1 firewall rule or use intra-zone traffic blocking to allow or block VPN traffic transmitting between the VPN tunnel and other interfaces in the LAN zone. If you add the VPN tunnel to a new zone (the VPN zone for example), you can configure rules for VPN traffic between the VPN zone and other zones or **From VPN To-Device** rules for VPN traffic destined for the ISG50.

Session Limits

Accessing the ISG50 or network resources through the ISG50 requires a NAT session and corresponding firewall session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the ISG50. The ISG50 lets you limit the number of concurrent NAT/firewall sessions a client can use.

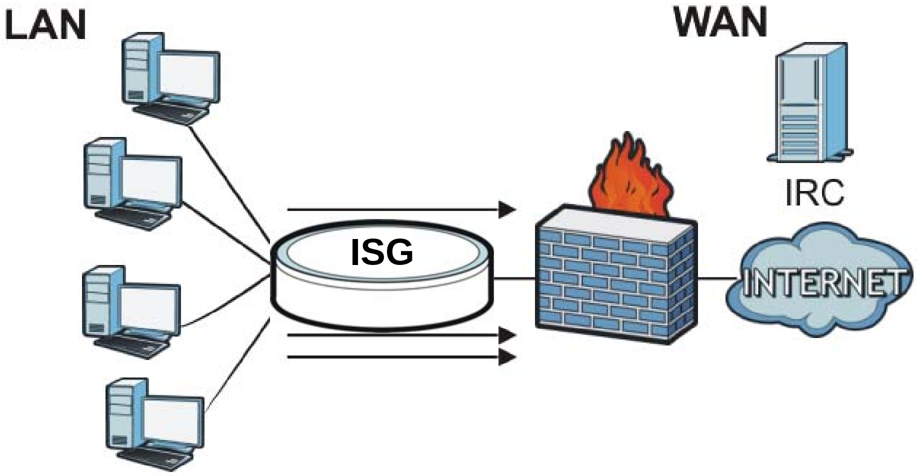
Finding Out More

- See Section 6.6.13 on page 101 for related information on the **Firewall** screens.
- See Section 7.8 on page 123 for an example of creating firewall rules as part of configuring user-aware access control (Section 7.5 on page 116).
- See Section 7.9.3 on page 128 for an example of creating a firewall rule to allow H.323 traffic from the WAN to the LAN.
- See Section 7.10.3 on page 131 for an example of creating a firewall rule to allow web traffic from the WAN to a server on the DMZ.

23.1.3 Firewall Rule Example Applications

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

Figure 234 Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following rules.

Table 114 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
2	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all LAN1 to WAN traffic.

The ISG50 applies the firewall rules in order. So for this example, when the ISG50 receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the second rule and the ISG50 forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN1 to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN rule that allows IRC traffic from any computer through which the CEO logs into the ISG50 with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

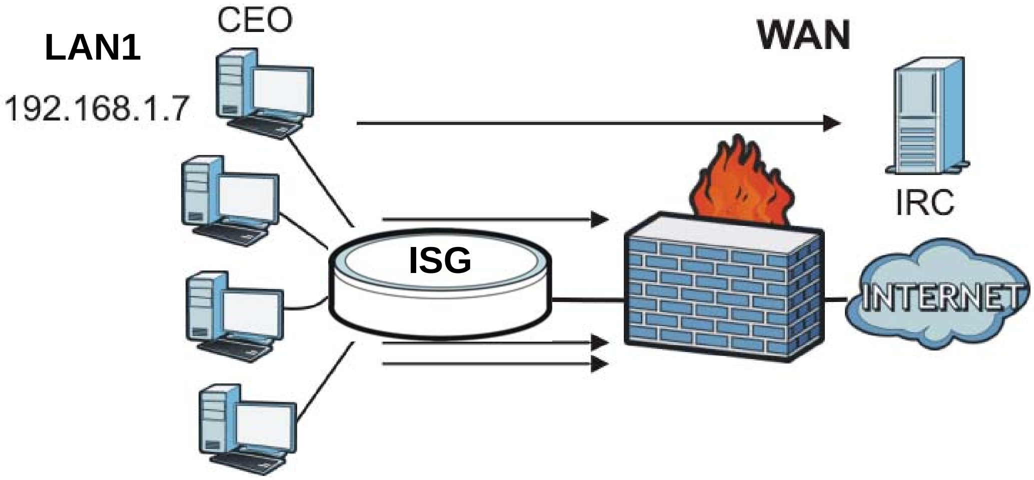
- Has a static IP address,

  or

- You configure a static DHCP entry for it so the ISG50 always assigns it the same IP address (see DHCP Settings on page 277 for information on DHCP).

Now you configure a LAN1 to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

Figure 235 Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 115 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN1 computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the firewall's default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN rule with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your firewall would have the following configuration.

Table 116 Limited LAN1 to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the ISG50 with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the firewall's default policy of allowing all traffic from the LAN1 to go to the WAN.

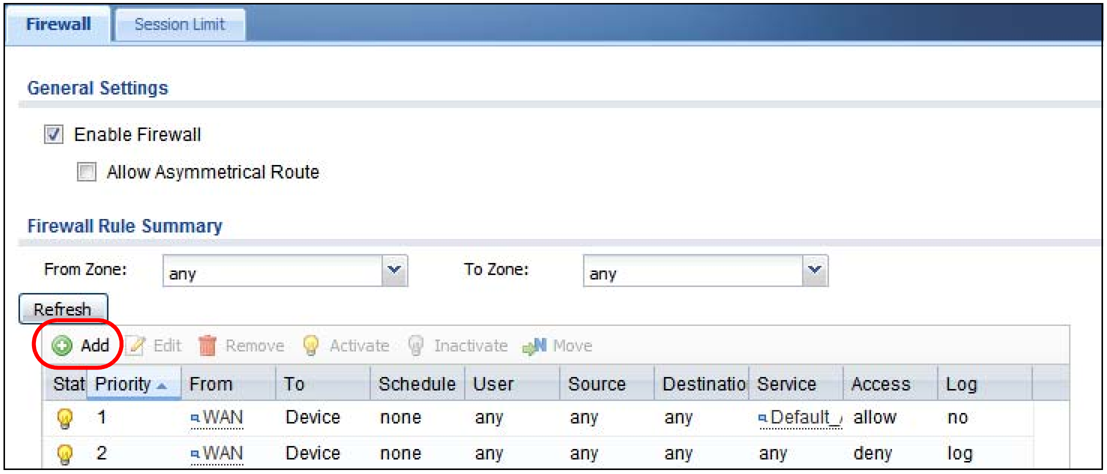
The rule for the CEO must come before the rule that blocks all LAN1 to WAN IRC traffic. If the rule that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ISG50 would drop it and not check any other firewall rules.

23.1.4 Firewall Rule Configuration Example

The following Internet firewall rule example allows Doom players from the WAN to IP addresses 192.168.1.10 through 192.168.1.15 (Dest_1) on the LAN1.

1 Click **Configuration > Firewall**. In the summary of firewall rules click **Add** in the heading row to configure a new first entry. Remember the sequence (priority) of the rules is important since they are applied in order.

Figure 236 Firewall Example: Firewall Screen



☑ Enable Firewall

☐ Allow Asymmetrical Route

From Zone: any

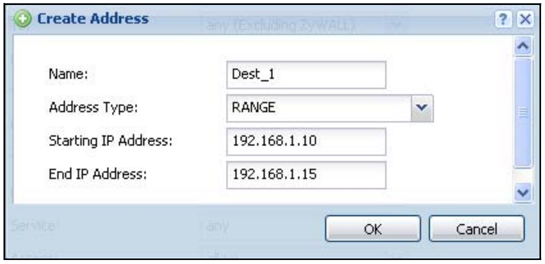
To Zone: any

Stat	Priority	From	To	Schedule	User	Source	Destinatio	Service	Access	Log
	1	WAN	Device	none	any	any	any	Default_	allow	no
	2	WAN	Device	none	any	any	any	any	deny	log

2 At the top of the screen, click **Create new Object > Address**.

3 The screen for configuring an address object opens. Configure it as follows and click **OK**.

Figure 237 Firewall Example: Create an Address Object



Name: Dest_1

Address Type: RANGE

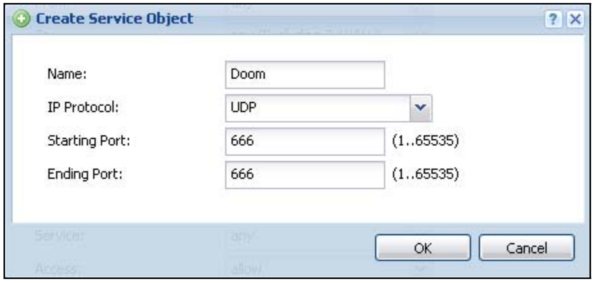
Starting IP Address: 192.168.1.10

End IP Address: 192.168.1.15

4 Click **Create new Object > Service**.

5 The screen for configuring a service object opens. Configure it as follows and click **OK**.

Figure 238 Firewall Example: Create a Service Object



Create Service Object
OK
Cancel

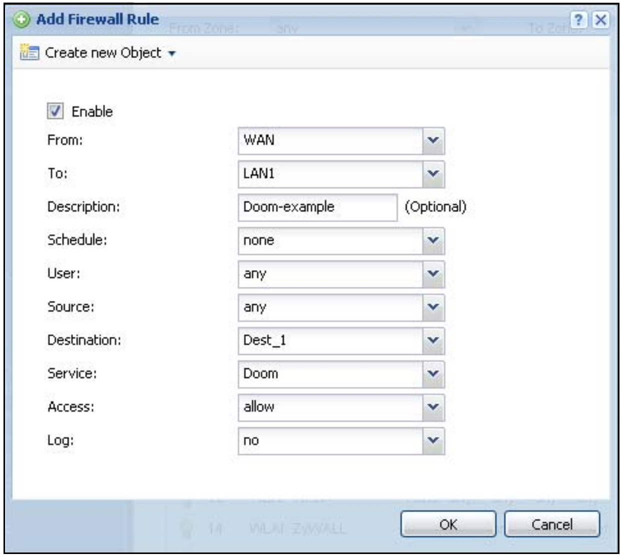
Name: Doom
IP Protocol: UDP
Starting Port: 666 (1..65535)
Ending Port: 666 (1..65535)

6 Select **From WAN** and **To LAN1**.

7 Enter the name of the firewall rule.

8 Select **Dest_1** is selected for the **Destination** and **Doom** is selected as the **Service**. Enter a description and configure the rest of the screen as follows. Click **OK** when you are done.

Figure 239 Firewall Example: Edit a Firewall Rule

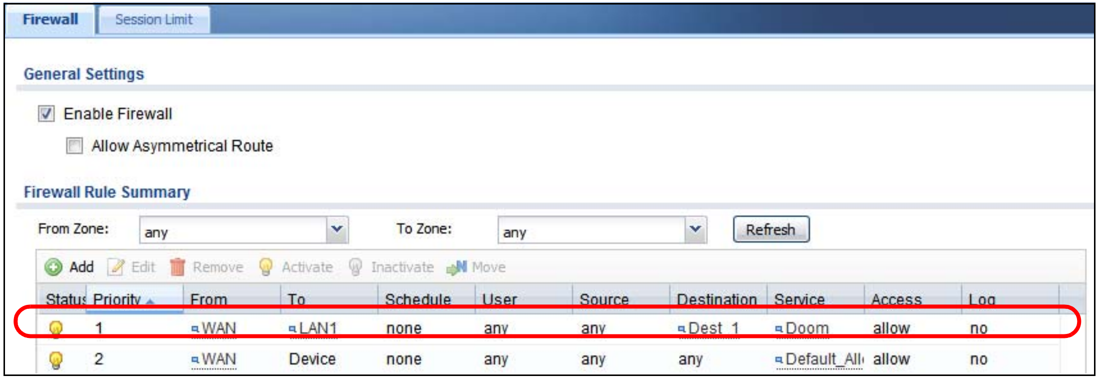


Add Firewall Rule
Create new Object
OK
Cancel

☑ Enable
From: WAN
To: LAN1
Description: Doom-example (Optional)
Schedule: none
User: any
Source: any
Destination: Dest_1
Service: Doom
Access: allow
Log: no

9 The firewall rule appears in the firewall rule summary.

Figure 240 Firewall Example: Doom Rule in Summary



Firewall
Session Limit
General Settings
Firewall Rule Summary
Refresh
Add
Edit
Remove
Activate
Inactivate
Move

☑ Enable Firewall
☐ Allow Asymmetrical Route

From Zone: any
To Zone: any

Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
	1	WAN	LAN1	none	any	any	Dest_1	Doom	allow	no
	2	WAN	Device	none	any	any	any	Default_All	allow	no

23.2 The Firewall Screen

Asymmetrical Routes

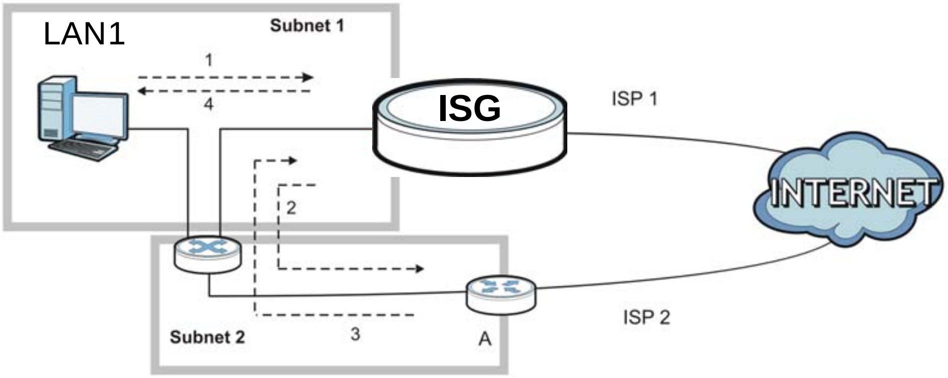
If an alternate gateway on the LAN has an IP address in the same subnet as the ISG50's LAN IP address, return traffic may not go through the ISG50. This is called an asymmetrical or "triangle" route. This causes the ISG50 to reset the connection, as the connection has not been acknowledged.

You can have the ISG50 permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ISG50. A better solution is to use virtual interfaces to put the ISG50 and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (**A** in the figure) in different subnets, all returning network traffic must pass through the ISG50 to the LAN. The following steps and figure describe such a scenario.

1. A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ISG50 reroutes the packet to gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the ISG50.
4. The ISG50 then sends it to the computer on the LAN1 in **Subnet 1**.

Figure 241 Using Virtual Interfaces to Avoid Asymmetrical Routes

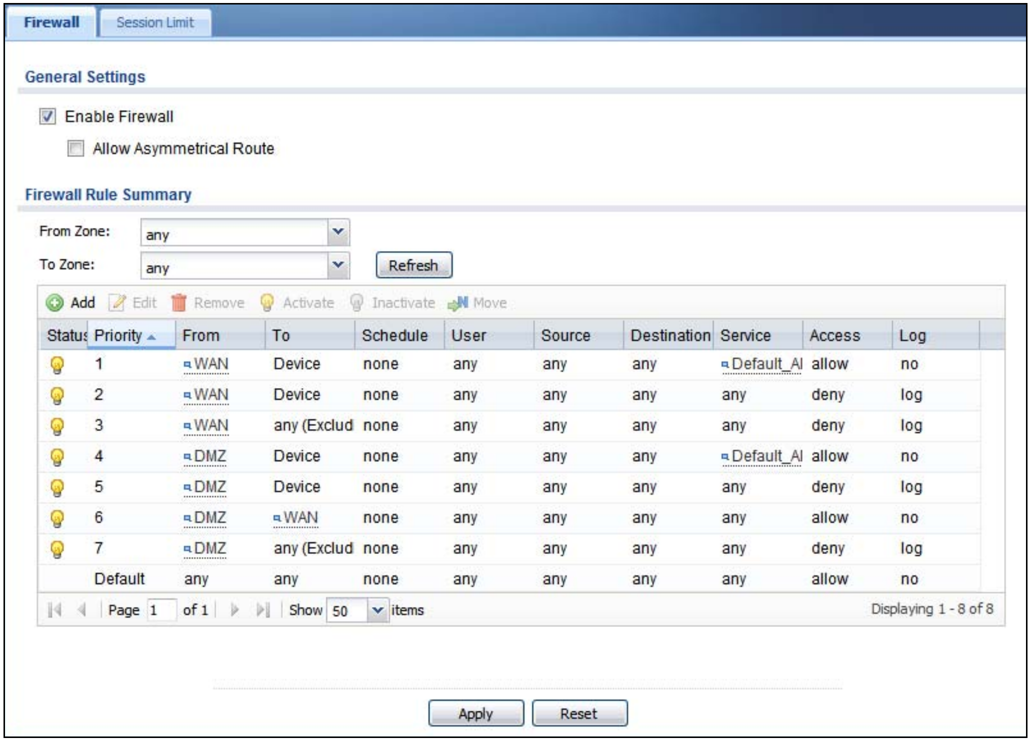


23.2.1 Configuring the Firewall Screen

Click **Configuration > Firewall** to open the **Firewall** screen. Use this screen to enable or disable the firewall and asymmetrical routes, set a maximum number of sessions per host, and display the configured firewall rules. Specify from which zone packets come and to which zone packets travel to display only the rules specific to the selected direction. Note the following.

- If you enable intra-zone traffic blocking (see the chapter about zones), the firewall automatically creates (implicit) rules to deny packet passage between the interfaces in the specified zone.
- Besides configuring the firewall, you also need to configure NAT rules to allow computers on the WAN to access LAN devices. See Chapter 18 on page 323 for more information.
- The ISG50 applies NAT (Destination NAT) settings before applying the firewall rules. So for example, if you configure a NAT entry that sends WAN traffic to a LAN IP address, when you configure a corresponding firewall rule to allow the traffic, you need to set the LAN IP address as the destination. See Section 7.9 on page 125 for an example.
- The ordering of your rules is very important as rules are applied in sequence.

Figure 242 Configuration > Firewall



☑ Enable Firewall

☐ Allow Asymmetrical Route

From Zone: any

To Zone: any

Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
💡	1	WAN	Device	none	any	any	any	Default_Al	allow	no
💡	2	WAN	Device	none	any	any	any	any	deny	log
💡	3	WAN	any (Exclud	none	any	any	any	any	deny	log
💡	4	DMZ	Device	none	any	any	any	Default_Al	allow	no
💡	5	DMZ	Device	none	any	any	any	any	deny	log
💡	6	DMZ	WAN	none	any	any	any	any	allow	no
💡	7	DMZ	any (Exclud	none	any	any	any	any	deny	log
	Default	any	any	none	any	any	any	any	allow	no

The following table describes the labels in this screen.

Table 117 Configuration > Firewall

LABEL	DESCRIPTION
General Settings	
Enable Firewall	Select this check box to activate the firewall. The ISG50 performs access control when the firewall is activated.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ISG50's LAN IP address, return traffic may not go through the ISG50. This is called an asymmetrical or "triangle" route. This causes the ISG50 to reset the connection, as the connection has not been acknowledged. Select this check box to have the ISG50 permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ISG50. A better solution is to use virtual interfaces to put the ISG50 and the backup gateway on separate subnets.
Firewall Rule Summary	

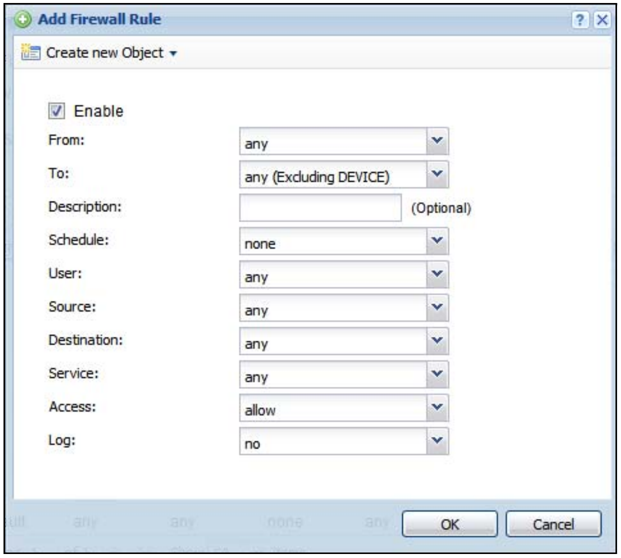
Table 117 Configuration > Firewall (continued)

LABEL	DESCRIPTION
From Zone / To Zone	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, from **LAN1** to **LAN1** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN1. From **any** displays all the firewall rules for traffic going to the selected **To Zone**. To **any** displays all the firewall rules for traffic coming from the selected **From Zone**. From **any** to **any** displays all of the firewall rules. To ISG50 rules are for traffic that is destined for the ISG50 and control which computers can manage the ISG50.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction.	
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of your firewall rule in the global rule list (including all through-ISG50 and to-ISG50 rules). The ordering of your rules is important as rules are applied in sequence. Default displays for the default firewall behavior that the ISG50 performs on traffic that does not match any other firewall rule.
From To	This is the direction of travel of packets to which the firewall rule applies.
Schedule	This field tells you the schedule object that the rule uses. **none** means the rule is active at all times if enabled.
User	This is the user name or user group name to which this firewall rule applies.
Source	This displays the source address object to which this firewall rule applies.
Destination	This displays the destination address object to which this firewall rule applies.
Service	This displays the service object to which this firewall rule applies.
Access	This field displays whether the firewall silently discards packets (**deny**), discards packets and sends a TCP reset packet to the sender (**reject**) or permits the passage of packets (**allow**).
Log	This field shows you whether a log (and alert) is created when packets match this rule or not.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

23.2.2 The Firewall Add/Edit Screen

In the **Firewall** screen, click the **Edit** or **Add** icon to display the **Firewall Rule Edit** screen.

Figure 243 Configuration > Firewall > Add



☑ Enable
From: any
To: any (Excluding DEVICE)
Description: (Optional)
Schedule: none
User: any
Source: any
Destination: any
Service: any
Access: allow
Log: no

The following table describes the labels in this screen.

Table 118 Configuration > Firewall > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to activate the firewall rule.
From To	For through-ISG50 rules, select the direction of travel of packets to which the rule applies. **any (Excluding DEVICE)** means all interfaces or VPN tunnels. **Device** means packets destined for the ISG50 itself.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the firewall rule. Spaces are allowed.
Schedule	Select a schedule that defines when the rule applies. Otherwise, select **none** and the rule is always effective.
User	This field is not available when you are configuring a to-ISG50 rule. Select a user name or user group to which to apply the rule. The firewall rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified a source IP address (group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Source	Select a source address or address group for whom this rule applies. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group for whom this rule applies. Select **any** if the policy is effective for every destination.
Service	Select a service or service group from the drop-down list box.

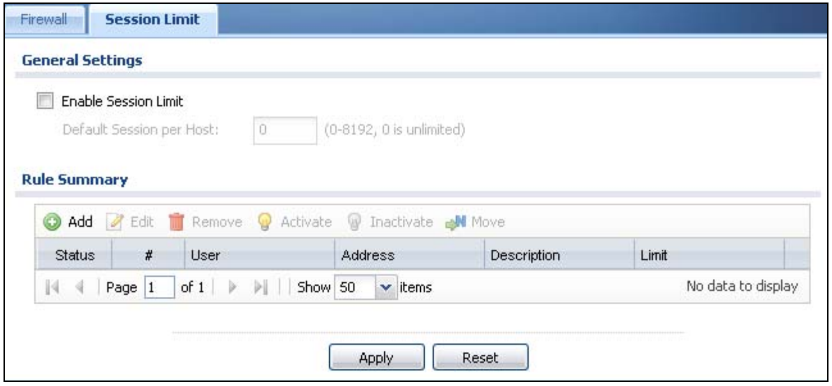
Table 118 Configuration > Firewall > Add (continued)

LABEL	DESCRIPTION
Access	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select **deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **reject** to deny the packets and send a TCP reset packet to the sender. Any UDP packets are dropped without sending a response packet. Select **allow** to permit the passage of the packets.
Log	Select whether to have the ISG50 generate a log (**log**), log and alert (**log alert**) or not (**no**) when the rule is matched. See Chapter 53 on page 705 for more on logs.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

23.3 The Session Limit Screen

Click **Configuration > Firewall > Session Limit** to display the **Firewall Session Limit** screen. Use this screen to limit the number of concurrent NAT/firewall sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

Figure 244 Configuration > Firewall > Session Limit



☐ Enable Session Limit

Default Session per Host: 0 (0-8192, 0 is unlimited)

Status	#	User	Address	Description	Limit

No data to display

The following table describes the labels in this screen.

Table 119 Configuration > Firewall > Session Limit

LABEL	DESCRIPTION
General Settings	
Enable Session limit	Select this check box to control the number of concurrent sessions hosts can have.
Default Session per Host	Use this field to set a common limit to the number of concurrent NAT/firewall sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. Create rules below to apply other limits for specific users or addresses.

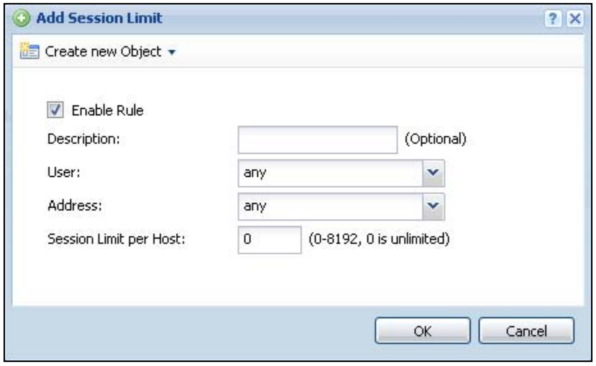
Table 119 Configuration > Firewall > Session Limit (continued)

LABEL	DESCRIPTION
Rule Summary	This table lists the rules for limiting the number of concurrent sessions hosts can have.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the index number of a session limit rule. It is not associated with a specific rule.
User	This is the user name or user group name to which this session limit rule applies.
Address	This is the address object to which this session limit rule applies.
Description	This displays the information entered to help identify this rule.
Limit	This is how many concurrent sessions this user or address is allowed to have.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

23.3.1 The Session Limit Add/Edit Screen

Click **Configuration > Firewall > Session Limit** and the **Add** or **Edit** icon to display the **Firewall Session Limit Edit** screen. Use this screen to configure rules that define a session limit for specific users or addresses.

Figure 245 Configuration > Firewall > Session Limit > Edit



☑ Enable Rule

Description: (Optional)

User: any

Address: any

Session Limit per Host: 0 (0-8192, 0 is unlimited)

The following table describes the labels in this screen.

Table 120 Configuration > Firewall > Session Limit > Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Select this check box to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 64 printable ASCII characters. Spaces are allowed.
User	Select a user name or user group to which to apply the rule. The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified an IP address (or address group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Address	Select a source address or address group for whom this rule applies. Select **any** if the policy is effective for every source address.
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/firewall sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the **Default Session per Host** setting in the general **Firewall Session Limit** screen.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

24

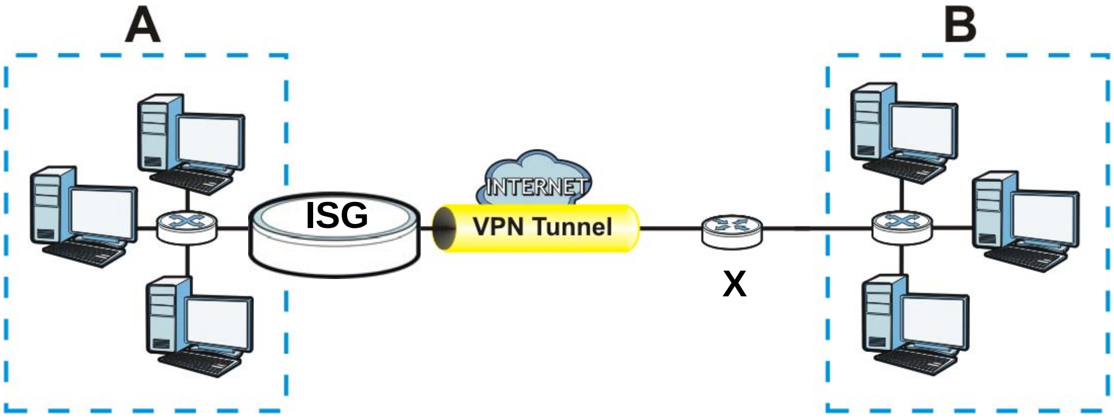
IPSec VPN

24.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The following figure is an example of an IPSec VPN tunnel.

Figure 246 IPSec VPN Example



The VPN tunnel connects the ISG50 and the remote (peer) IPSec router (**X**). These routers then connect the local network (**A**) and remote network (**B**).

Note: You can use a subscription to increase the number of supported IPSec VPN tunnels. See Chapter 11 on page 229.

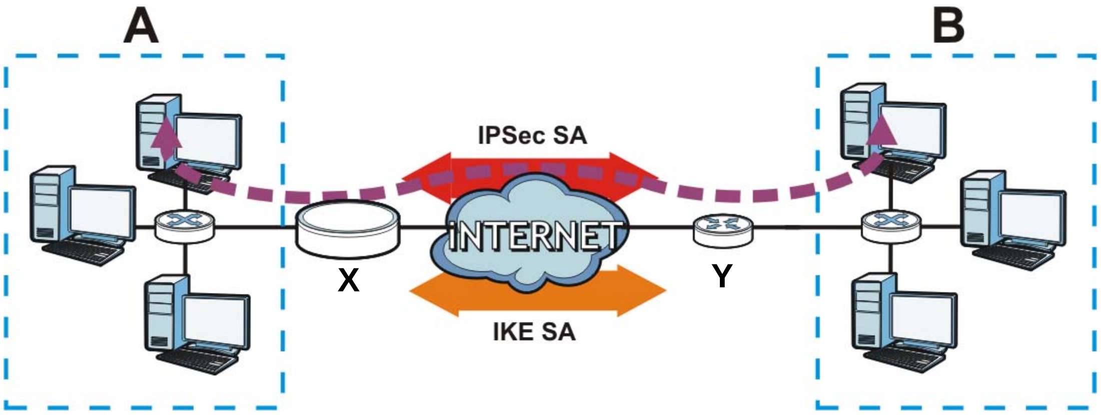
24.1.1 What You Can Do in this Chapter

- Use the **VPN Connection** screens (see Section 24.2 on page 370) to specify which VPN gateway a VPN connection policy uses and which devices (behind the IPSec routers) can use the VPN tunnel and the IPSec SA settings (phase 2 settings). You can also activate / deactivate and connect / disconnect each VPN connection (each IPSec SA).
- Use the **VPN Gateway** screens (see Section 24.2.1 on page 371) to manage the ISG50's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.

24.1.2 What You Need to Know

An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ISG50 and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ISG50 and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ISG50 and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 247 VPN: IKE SA and IPSec SA

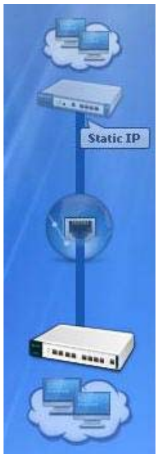
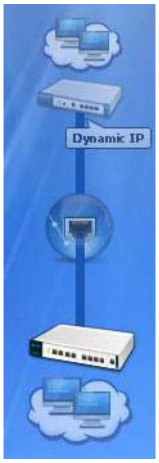
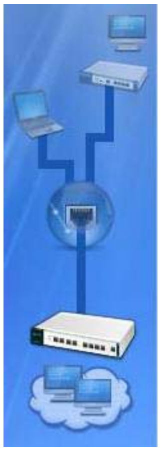
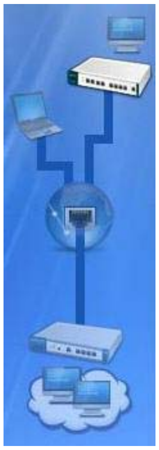


In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

Application Scenarios

The ISG50's application scenarios make it easier to configure your VPN connection settings.

Table 121 IPSec VPN Application Scenarios

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER	REMOTE ACCESS (SERVER ROLE)	REMOTE ACCESS (CLIENT ROLE)
			
Choose this if the remote IPSec router has a static IP address or a domain name. For example, a branch office with an ISG50 or a VPN router with a static IP address. This ISG50 can initiate the VPN tunnel. The remote IPSec router can also initiate the VPN tunnel if this ISG50 has a static IP address or a domain name.	Choose this if the remote IPSec router has a dynamic IP address. For example, a branch office with an ISG50 or a VPN router with a dynamic IP address. You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router). This ISG50 must have a static IP address or a domain name. Only the remote IPSec router can initiate the VPN tunnel.	Choose this to allow incoming connections from IPSec VPN clients, including smartphone applications. Smartphone applications require a valid subscription to use. See Chapter 11 on page 229. The clients have dynamic IP addresses and are also known as dial-in users. You don't specify the addresses of the client IPSec routers or the remote policy. This creates a dynamic IPSec VPN rule that can let multiple clients connect. Only the clients can initiate the VPN tunnel.	Choose this to connect to an IPSec server. This ISG50 is the client (dial-in user). Client role ISG50s initiate IPSec VPN connections to a server role ISG50. This ISG50 can have a dynamic IP address. The IPSec server doesn't configure this ISG50's IP address or the addresses of the devices behind it. Only this ISG50 can initiate the VPN tunnel.

Finding Out More

- See Section 6.6.14 on page 102 for related information on these screens.
- See Section 24.4 on page 386 for IPSec VPN background information.
- See Section 5.4 on page 77 for the IPSec VPN quick setup wizard.
- See Section 7.4 on page 113 for an example of configuring IPSec VPN.

24.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

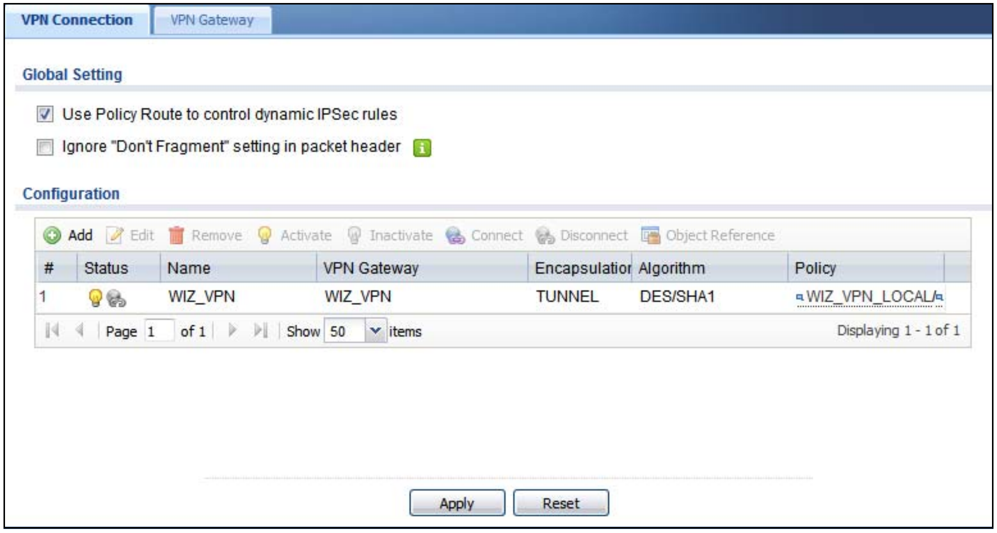
You should set up the following features before you set up the VPN tunnel.

- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the ISG50 uses as its IP address when it establishes the IKE SA. You should set up the interface first. See Chapter 12 on page 233.
- In a VPN gateway, you can enable extended authentication. If the ISG50 is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the ISG50 authenticates the remote IPSec router. See Chapter 48 on page 631.
- In a VPN gateway, the ISG50 and remote IPSec router can use certificates to authenticate each other. Make sure the ISG50 and the remote IPSec router will trust each other's certificates. See Chapter 50 on page 643.

24.2 The VPN Connection Screen

Click **Configuration > VPN > IPSec VPN** to open the **VPN Connection** screen. The **VPN Connection** screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate / deactivate and connect / disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 248 Configuration > VPN > IPSec VPN > VPN Connection



Global Setting

☑ Use Policy Route to control dynamic IPSec rules

☐ Ignore "Don't Fragment" setting in packet header

Configuration

#	Status	Name	VPN Gateway	Encapsulatio	Algorithm	Policy
1		WIZ_VPN	WIZ_VPN	TUNNEL	DES/SHA1	WIZ_VPN_LOCAL/

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Each field is discussed in the following table. See Section 24.2.2 on page 377 and Section 24.2.1 on page 371 for more information.

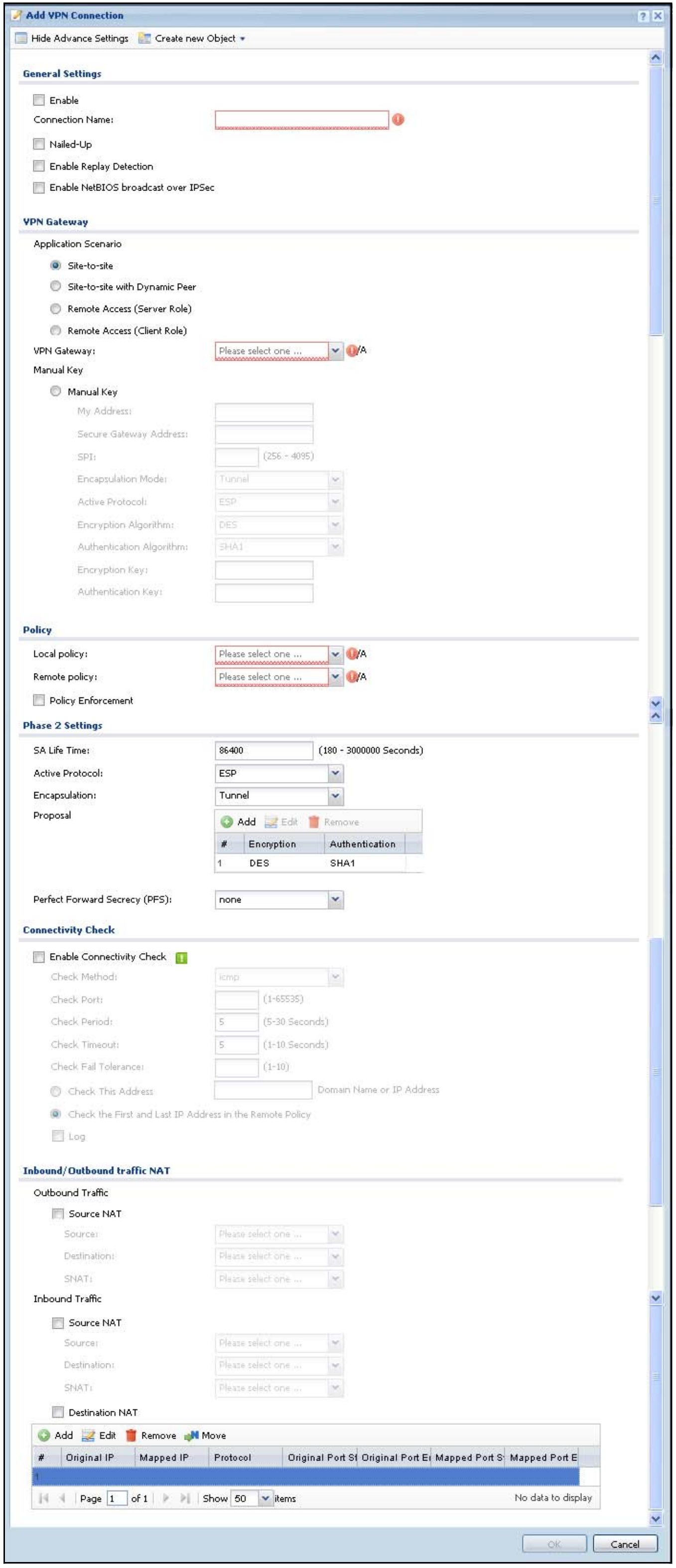
Table 122 Configuration > VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
Use Policy Route to control dynamic IPSec rules	Select this to be able to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The ISG50 automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. Clear this to have the ISG50 automatically obtain source and destination addresses for all dynamic IPSec rules. See Section 6.5.1 on page 95 for how this option affects the routing table.
Ignore ""Don't Fragment"" setting in packet header	Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the “don’t” fragment” bit in the IP header turned on. When you clear this the ISG50 drops packets larger than the MTU that have the “don’t” fragment” bit in the header turned on.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an IPSec SA, select it and click **Connect**.
Disconnect	To disconnect an IPSec SA, select it and click **Disconnect**.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific connection.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the IPSec SA.
VPN Gateway	This field displays the associated VPN gateway(s). If there is no VPN gateway, this field displays “manual key”.
Encapsulation	This field displays what encapsulation the IPSec SA uses.
Algorithm	This field displays what encryption and authentication methods, respectively, the IPSec SA uses.
Policy	This field displays the local policy and the remote policy, respectively.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

24.2.1 The VPN Connection Add/Edit (IKE) Screen

The **VPN Connection Add/Edit Gateway** screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the **Configuration > VPN Connection** screen (see Section 24.2 on page 370), and click either the **Add** icon or an **Edit** icon. If you click the **Add** icon, you have to select a specific VPN gateway in the **VPN Gateway** field before the following screen appears.

Figure 249 Configuration > VPN > IPSec VPN > VPN Connection > Edit (IKE)



General Settings

☐ Enable
Connection Name:
☐ Nailed-Up
☐ Enable Replay Detection
☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario
● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)
VPN Gateway: Please select one ... /A
Manual Key
○ Manual Key
My Address:
Secure Gateway Address:
SPI: (256 - 4095)
Encapsulation Mode: Tunnel
Active Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: SHA1
Encryption Key:
Authentication Key:

Policy

Local policy: Please select one ... /A
Remote policy: Please select one ... /A
☐ Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)
Active Protocol: ESP
Encapsulation: Tunnel
Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Connectivity Check

☐ Enable Connectivity Check
Check Method: icmp
Check Port: (1-65535)
Check Period: 5 (5-30 Seconds)
Check Timeout: 5 (1-10 Seconds)
Check Fail Tolerance: (1-10)
○ Check This Address Domain Name or IP Address
● Check the First and Last IP Address in the Remote Policy
☐ Log

Inbound/Outbound traffic NAT

Outbound Traffic
☐ Source NAT
Source: Please select one ...
Destination: Please select one ...
SNAT: Please select one ...
Inbound Traffic
☐ Source NAT
Source: Please select one ...
Destination: Please select one ...
SNAT: Please select one ...
☐ Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port St	Original Port En	Mapped Port St	Mapped Port E
1							

Page 1 of 1 | Show 50 items | No data to display

Each field is described in the following table.

Table 123 Configuration > VPN > IPSec VPN > VPN Connection > Edit

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this check box to activate this VPN connection.
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed-Up	Select this if you want the ISG50 to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	Select this check box if you the ISG50 to send NetBIOS (Network Basic Input/ Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
VPN Gateway	
Application Scenario	Select the scenario that best describes your intended VPN connection. **Site-to-site** - Choose this if the remote IPSec router has a static IP address or a domain name. This ISG50 can initiate the VPN tunnel. **Site-to-site with Dynamic Peer** - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. **Remote Access (Server Role)** - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. **Remote Access (Client Role)** - Choose this to connect to an IPSec server. This ISG50 is the client (dial-in user) and can initiate the VPN tunnel.
VPN Gateway	Select the VPN gateway this VPN connection is to use or select **Create Object** to add another VPN gateway for this VPN connection to use.
Manual Key	Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management. See Section 24.2.2 on page 377 for how to configure the manual key fields. Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.
Policy	
Local Policy	Select the address corresponding to the local network. Use **Create new Object** if you need to configure a new one.
Remote Policy	Select the address corresponding to the remote network. Use **Create new Object** if you need to configure a new one.

Table 123 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Policy Enforcement	Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks. Selecting this restricts who can use the VPN tunnel. The ISG50 drops traffic with source and destination IP addresses that do not match the local and remote policy.
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The ISG50 automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication** algorithm. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption** algorithm and **Authentication** algorithm. Both **AH** and **ESP** increase processing requirements and latency (delay). The ISG50 and remote IPSec router must use the same active protocol.
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data. **Transport** - this mode only encrypts the data. The ISG50 and remote IPSec router must use the same encapsulation.
Proposal	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ISG50 and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.

Table 123 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower. The ISG50 and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **none** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number **DH5** - enable PFS and use a 1536-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Connectivity Check	The ISG50 can regularly check the VPN connection to the gateway you specified to make sure it is still available.
Enable Connectivity Check	Select this to turn on the VPN connection check.
Check Method	Select how the ISG50 checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the ISG50 regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** to have the ISG50 regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection.
Check Port	This field displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures allowed before the ISG50 disconnects the VPN tunnel. The ISG50 resumes using the first peer gateway address when the VPN connection passes the connectivity check.
Check this Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check the First and Last IP Address in the Remote Policy	Select this to have the ISG50 check the connection to the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address.
Log	Select this to have the ISG50 generate a log every time it checks this VPN connection.
Inbound/Outbound traffic NAT	
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the ISG50 to route packets from computers outside the local network through the IPSec SA.

Table 123 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address object for the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the remote network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the local network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address that hides the original source address. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, or **All**.
Original Port Start / Original Port End	These fields are available if the protocol is **TCP** or **UDP**. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port Start / Mapped Port End	These fields are available if the protocol is **TCP** or **UDP**. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.

Table 123 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

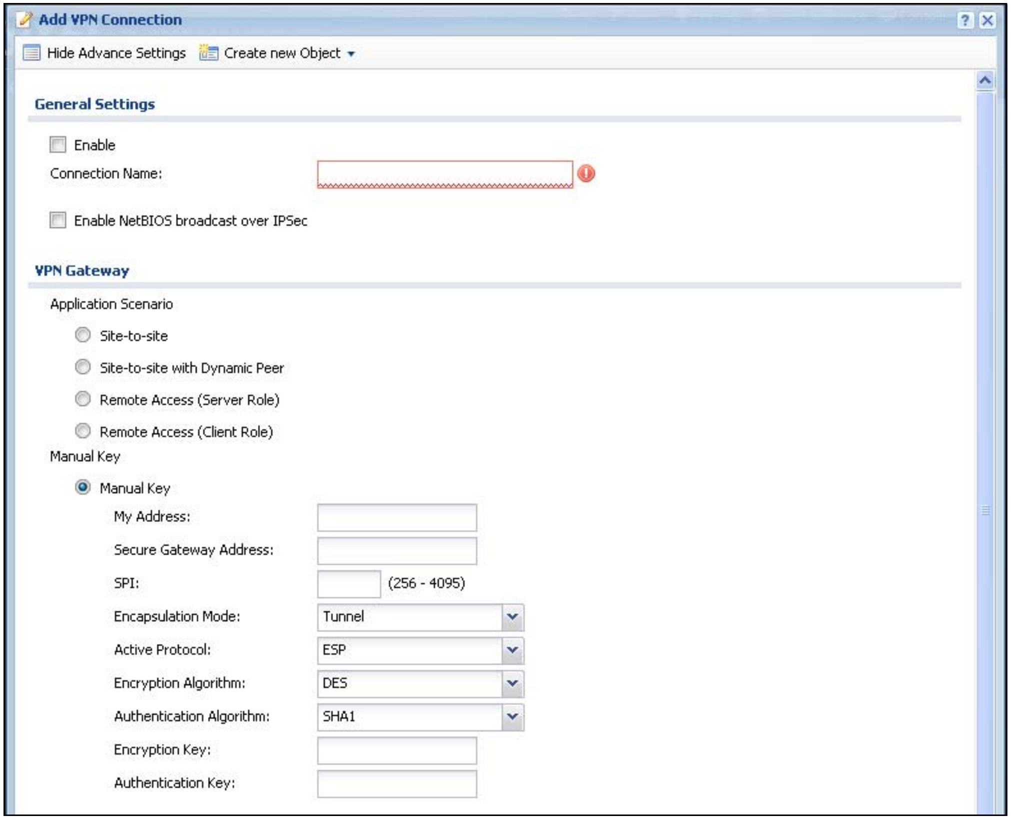
LABEL	DESCRIPTION
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

24.2.2 The VPN Connection Add/Edit Manual Key Screen

The **VPN Connection Add/Edit Manual Key** screen allows you to create a new VPN connection or edit an existing one using a manual key. This is useful if you have problems with IKE key management. To access this screen, go to the **VPN Connection summary** screen (see Section 24.2 on page 370), and click either the **Add** icon or an existing manual key entry's **Edit** icon. In the VPN Gateway section of the screen, select **Manual Key**.

Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.

Figure 250 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key



General Settings

☐ Enable

Connection Name:

☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

○ Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

Manual Key

● Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Encryption Key:

Authentication Key:

This table describes labels specific to manual key configuration. See Section 24.2 on page 370 for descriptions of the other fields.

Table 124 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key

LABEL	DESCRIPTION
Manual Key	
My Address	Type the IP address of the ISG50 in the IPSec SA. 0.0.0.0 is invalid.

Table 124 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key (continued)

LABEL	DESCRIPTION
Secure Gateway Address	Type the IP address of the remote IPSec router in the IPSec SA.
SPI	Type a unique **SPI** (Security Parameter Index) between 256 and 4095. The SPI is used to identify the ISG50 during authentication. The ISG50 and remote IPSec router must use the same SPI.
Encapsulation Mode	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data **Transport** - this mode only encrypts the data. You should only select this if the IPSec SA is used for communication between the ISG50 and remote IPSec router. If you select **Transport** mode, the ISG50 automatically switches to **Tunnel** mode if the IPSec SA is not used for communication between the ISG50 and remote IPSec router. In this case, the ISG50 generates a log message for this change. The ISG50 and remote IPSec router must use the same encapsulation.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication Algorithm**. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption Algorithm** and **Authentication Algorithm**. The ISG50 and remote IPSec router must use the same protocol.
Encryption Algorithm	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ISG50 and the remote IPSec router must use the same algorithm and key. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower. The ISG50 and remote IPSec router must use the same algorithm.

Table 124 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key (continued)

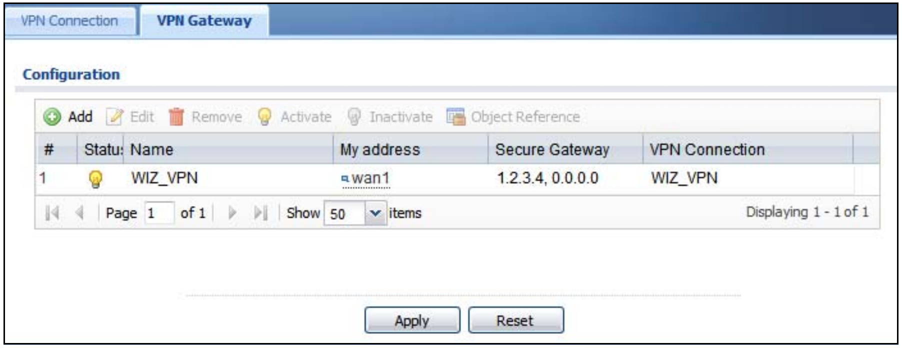
LABEL	DESCRIPTION
Encryption Key	This field is applicable when you select an **Encryption Algorithm**. Enter the encryption key, which depends on the encryption algorithm. **DES** - type a unique key 8-32 characters long **3DES** - type a unique key 24-32 characters long **AES128** - type a unique key 16-32 characters long **AES192** - type a unique key 24-32 characters long **AES256** - type a unique key 32 characters long You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The remote IPSec router must have the same encryption key. The ISG50 ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ISG50 only uses 12345678. The ISG50 still stores the longer key.
Authentication Key	Enter the authentication key, which depends on the authentication algorithm. **MD5** - type a unique key 16-20 characters long **SHA1** - type a unique key 20 characters long You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The remote IPSec router must have the same authentication key. The ISG50 ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 12345678901234567890 for a MD5 authentication key, the ISG50 only uses 1234567890123456. The ISG50 still stores the longer key.
OK	Click **OK** to save your settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

24.3 The VPN Gateway Screen

The **VPN Gateway** summary screen displays the IPSec VPN gateway policies in the ISG50, as well as the ISG50’s address, remote IPSec router’s address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway.

To access this screen, click **Configuration > VPN** > **Network** > **IPSec VPN** > **VPN Gateway**. The following screen appears.

Figure 251 Configuration > VPN > IPSec VPN > VPN Gateway



#	Statu:	Name	My address	Secure Gateway	VPN Connection
1	💡	WIZ_VPN	wan1	1.2.3.4, 0.0.0.0	WIZ_VPN

Each field is discussed in the following table. See Section 24.3.1 on page 381 for more information.

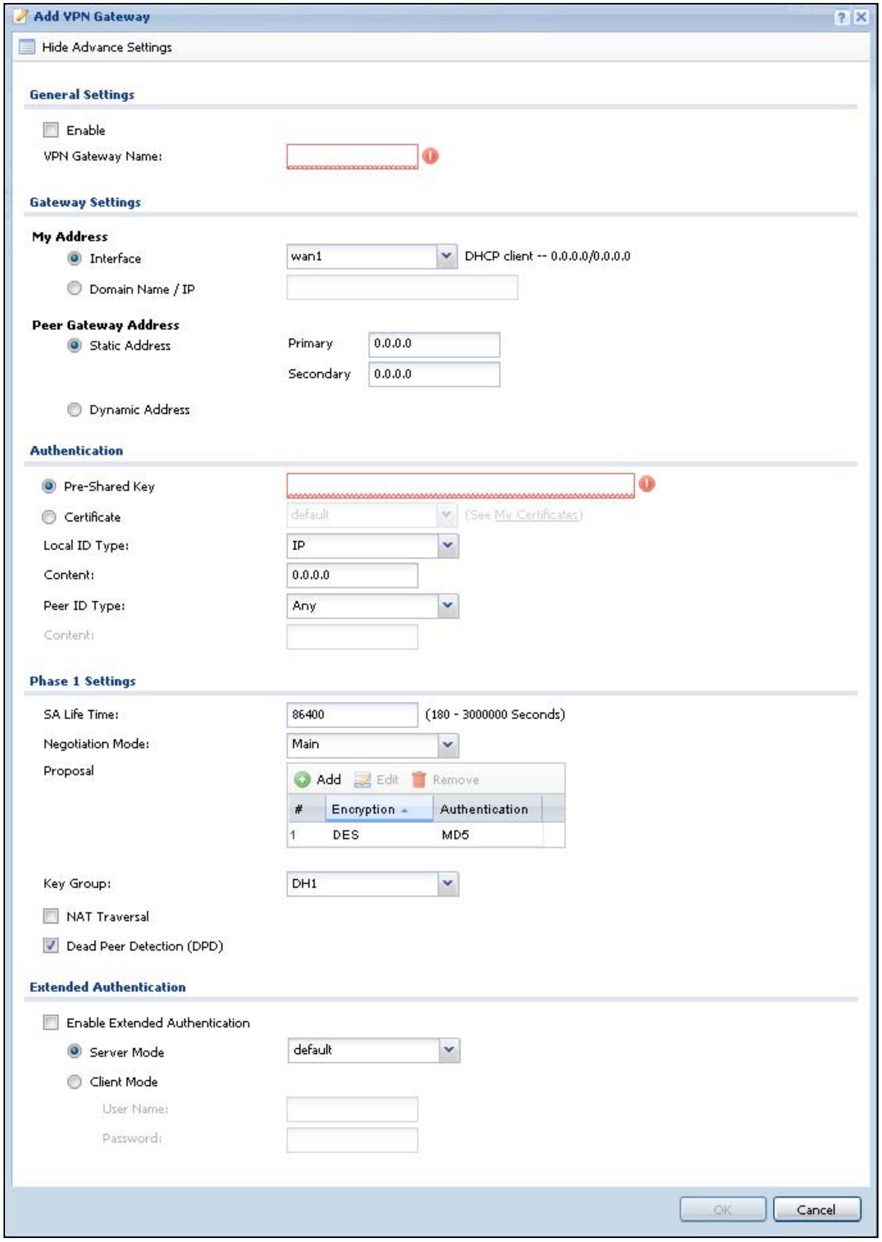
Table 125 Configuration > VPN > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific VPN gateway.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VPN gateway
My address	This field displays the interface or a domain name the ISG50 uses for the VPN gateway.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

24.3.1 The VPN Gateway Add/Edit Screen

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the **VPN Gateway summary** screen (see Section 24.3 on page 379), and click either the **Add** icon or an **Edit** icon.

Figure 252 Configuration > VPN > IPSec VPN > VPN Gateway > Edit



General Settings

☐ Enable

VPN Gateway Name:

Gateway Settings

My Address

● Interface: wan1 DHCP client -- 0.0.0.0/0.0.0.0

○ Domain Name / IP

Peer Gateway Address

● Static Address: Primary 0.0.0.0, Secondary 0.0.0.0

○ Dynamic Address

Authentication

● Pre-Shared Key

○ Certificate: default (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal: Add Edit Remove

#	Encryption	Authentication
1	DES	MD5

Key Group: DH1

☐ NAT Traversal

☑ Dead Peer Detection (DPD)

Extended Authentication

☐ Enable Extended Authentication

● Server Mode: default

○ Client Mode

User Name:

Password:

Each field is described in the following table.

Table 126 Configuration > VPN > IPSec VPN > VPN Gateway > Edit

LABEL	DESCRIPTION
Show Advance Settings / Hide Advance Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Gateway Settings	
My Address	Select how the IP address of the ISG50 in the IKE SA is defined. If you select **Interface**, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface or PPPoE/PPTP interface. The IP address of the ISG50 in the IKE SA is the IP address of the interface. If you select **Domain Name / IP**, enter the domain name or the IP address of the ISG50. The IP address of the ISG50 in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is invalid.
Peer Gateway Address	Select how the IP address of the remote IPSec router in the IKE SA is defined. Select **Static Address** to enter the domain name or the IP address of the remote IPSec router. You can provide a second IP address or domain name for the ISG50 to try if it cannot establish an IKE SA with the first one. Select **Dynamic Address** if the remote IPSec router has a dynamic IP address (and does not use DDNS).
Authentication	Note: The ISG50 and remote IPSec router must use the same authentication method to establish the IKE SA.
Pre-Shared Key	Select this to have the ISG50 and remote IPSec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be • 8 - 32 alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • 8 - 32 pairs of hexadecimal (0-9, A-F) characters, preceded by “0x”. If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs. The ISG50 and remote IPSec router must use the same pre-shared key.
Certificate	Select this to have the ISG50 and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the ISG50 uses to identify itself to the remote IPsec router. This certificate is one of the certificates in **My Certificates**. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA. Note: The IPSec routers must trust each other’s certificates. The ISG50 uses one of its **Trusted Certificates** to authenticate the remote IPSec router’s certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router’s certificate.

Table 126 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Local ID Type	This field is read-only if the ISG50 and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the ISG50 during authentication. Choices are: **IP** - the ISG50 is identified by an IP address **DNS** - the ISG50 is identified by a domain name **E-mail** - the ISG50 is identified by an e-mail address
Content	This field is read-only if the ISG50 and remote IPSec router use certificates to identify each other. Type the identity of the ISG50 during authentication. The identity depends on the **Local ID Type**. **IP** - type an IP address; if you type 0.0.0.0, the ISG50 uses the IP address specified in the **My Address** field. This is not recommended in the following situations: • There is a NAT router between the ISG50 and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Local ID Type**. **DNS** - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. **E-mail** - the ISG50 is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.
Peer ID Type	Select which type of identification is used to identify the remote IPSec router during authentication. Choices are: **IP** - the remote IPSec router is identified by an IP address **DNS** - the remote IPSec router is identified by a domain name **E-mail** - the remote IPSec router is identified by an e-mail address **Any** - the ISG50 does not check the identity of the remote IPSec router If the ISG50 and remote IPSec router use certificates, there is one more choice. **Subject Name** - the remote IPSec router is identified by the subject name in the certificate

Table 126 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Content	This field is disabled if the **Peer ID Type** is **Any**. Type the identity of the remote IPSec router during authentication. The identity depends on the **Peer ID Type**. If the ISG50 and remote IPSec router do not use certificates, **IP** - type an IP address; see the note at the end of this description. **DNS** - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. **E-mail** - the ISG50 is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. If the ISG50 and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router. **IP** - subject alternative name field; see the note at the end of this description. **DNS** - subject alternative name field **E-mail** - subject alternative name field **Subject Name** - subject name (maximum 255 ASCII characters, including spaces) Note: If **Peer ID Type** is **IP**, please read the rest of this section. If you type 0.0.0.0, the ISG50 uses the IP address specified in the **Secure Gateway Address** field. This is not recommended in the following situations: • There is a NAT router between the ISG50 and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Peer ID Type**.
Phase 1 Settings	
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the ISG50 and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Negotiation Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are **Main** - this encrypts the ISG50's and remote IPSec router's identities but takes more time to establish the IKE SA **Aggressive** - this is faster but does not encrypt the identities The ISG50 and the remote IPSec router must use the same negotiation mode.
Proposal	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.

Table 126 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ISG50 and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol. • There are one or more NAT routers between the ISG50 and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.
Dead Peer Detection (DPD)	Select this check box if you want the ISG50 to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the ISG50 sends a message to the remote IPSec router. If the remote IPSec router responds, the ISG50 transmits the data. If the remote IPSec router does not respond, the ISG50 shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 24.2.1 on page 371).
Extended Authentication	When multiple IPSec routers use the same VPN tunnel to connect to a single VPN tunnel (telecommuters sharing a tunnel for example), use extended authentication to enforce a user name and password check. This way even though they all know the VPN tunnel’s security settings, each still has to provide a unique user name and password.

Table 126 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Enable Extended Authentication	Select this if one of the routers (the ISG50 or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server.
Server Mode	Select this if the ISG50 authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the ISG50 authenticates this information.
Client Mode	Select this radio button if the ISG50 provides a username and password to the remote IPSec router for authentication. You also have to provide the **User Name** and the **Password**.
User Name	This field is required if the ISG50 is in **Client Mode** for extended authentication. Type the user name the ISG50 sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the ISG50 is in **Client Mode** for extended authentication. Type the password the ISG50 sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
OK	Click **OK** to save your settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

24.4 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

IKE SA Overview

The IKE SA provides a secure connection between the ISG50 and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 389. Main mode is used in various examples in the rest of this section.

IP Addresses of the ISG50 and Remote IPSec Router

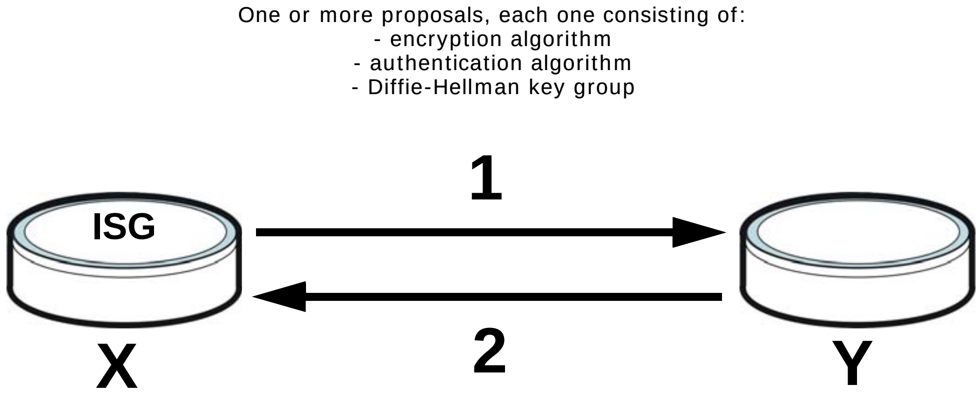
To set up an IKE SA, you have to specify the IP addresses of the ISG50 and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your ISG50 might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the ISG50 does not know the IP address of the remote IPSec router. This is often used for telecommuters.

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ISG50 and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 253 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal


One or more proposals, each one consisting of:
- encryption algorithm
- authentication algorithm
- Diffie-Hellman key group
1
ISG
2
X
Y

The ISG50 sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ISG50 wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ISG50. If the remote IPSec router rejects all of the proposals, the ISG50 and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most ISG50s, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some ISG50s also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most ISG50s, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

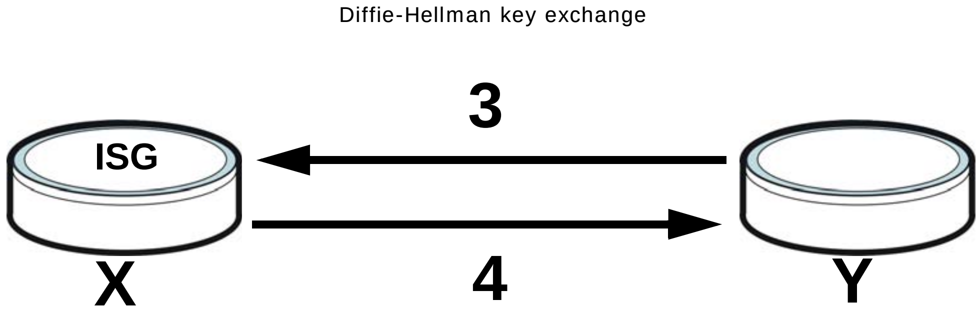
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

See Diffie-Hellman (DH) Key Exchange on page 388 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The ISG50 and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 254 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange


Diffie-Hellman key exchange
3
ISG
X
4
Y

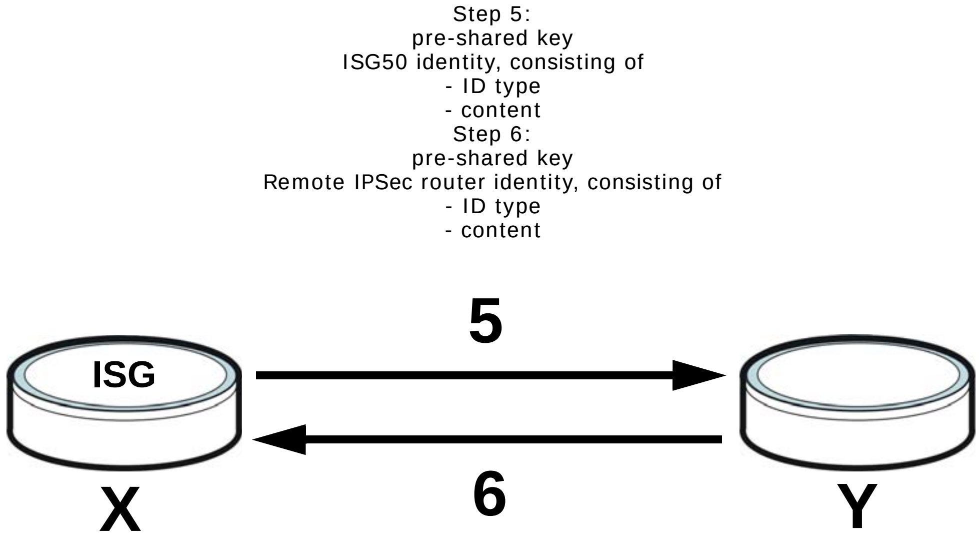
DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Authentication

Before the ISG50 and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ISG50 and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the ISG50 and remote IPSec router selected in previous steps.

Figure 255 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)


Step 5:
pre-shared key
ISG50 identity, consisting of
- ID type
- content
Step 6:
pre-shared key
Remote IPSec router identity, consisting of
- ID type
- content
5
ISG
X
6
Y

You have to create (and distribute) a pre-shared key. The ISG50 and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

Note: The ISG50 and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any domain name or e-mail address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the ISG50's or remote IPSec router's properties.

The ISG50 and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The ISG50's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in Table 127 on page 389, the ISG50 and the remote IPSec router authenticate each other successfully. In contrast, in Table 128 on page 389, the ISG50 and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 127 VPN Example: Matching ID Type and Content

ISG50	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

Table 128 VPN Example: Mismatching ID Type and Content

ISG50	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the ISG50 to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your ISG50 provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The ISG50 sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ISG50.

Steps 3 - 4: The ISG50 and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

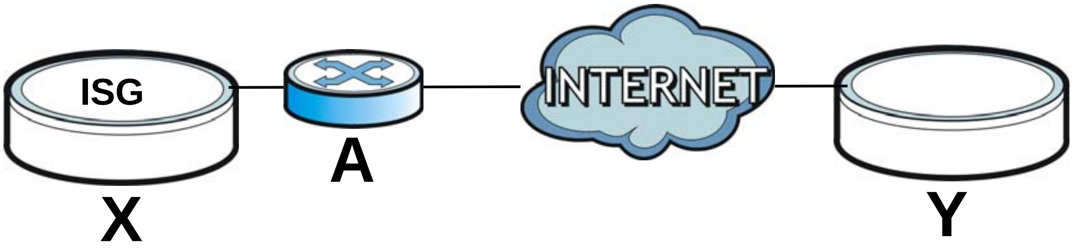
Steps 5 - 6: Finally, the ISG50 and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the ISG50 and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 256 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Active Protocol on page 392 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ISG50 and remote IPSec router.

- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ISG50 and remote IPSec router support.

Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the ISG50 or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ISG50 to provide a user name and password to the remote IPSec router, or you can set up the ISG50 to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

Certificates

It is possible for the ISG50 and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the ISG50 and remote IPSec router check the signatures on each other’s certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the ISG50 and remote IPSec router first.

IPSec SA Overview

Once the ISG50 and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the ISG50, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The ISG50 and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

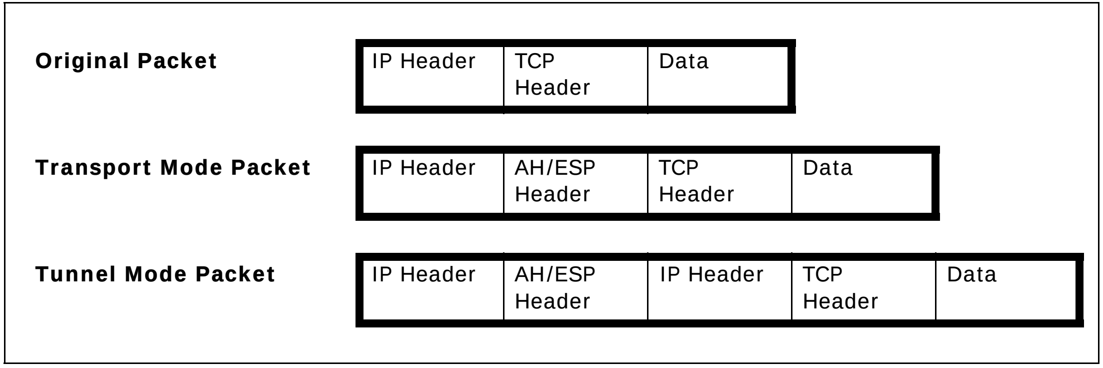
Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the ISG50 and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The ISG50 and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 257 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the ISG50 uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ISG50 or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ISG50 or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ISG50 includes part of the original IP header when it encapsulates the packet. With ESP, however, the ISG50 does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal on page 387), except that you also have the choice whether or not the ISG50 and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ISG50 and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the ISG50 and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

Additional Topics for IPSec SA

This section provides more information about IPSec SA in your ISG50.

IPSec SA using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the ISG50 and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

IPSec SA Proposal using Manual Keys

In an IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ISG50 and remote IPSec router use.

Note: The ISG50 and remote IPSec router must use the same encryption key and authentication key.

Authentication and the Security Parameter Index (SPI)

For authentication, the ISG50 and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The ISG50 and remote IPSec router must use the same SPI.

NAT for Inbound and Outbound Traffic

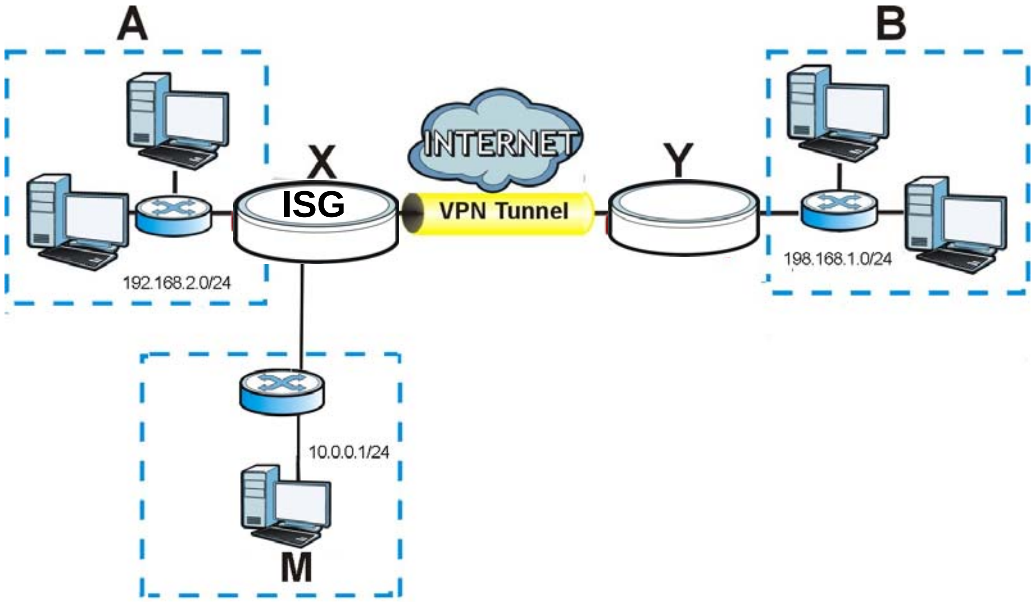
The ISG50 can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the ISG50 to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.

- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 258 VPN Example: NAT for Inbound and Outbound Traffic



Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the ISG50 route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 258 on page 394, you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPSec router may not route messages for computer **M** through the IPSec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.
- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).
- Destination - the original destination address; the local network (**A**).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the ISG50 to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 258 on page 394, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The ISG50 checks these rules similar to the way it checks rules for a firewall. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 258 on page 394, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

- Mapped IP - the translated destination address; in Figure 258 on page 394, the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

25

Bandwidth Management

25.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

25.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see Section 25.2 on page 404) to control bandwidth for services passing through the ISG50, and it identifies the conditions that refine this.

25.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over policy routes to manage the bandwidth of TCP and UDP traffic.

If you want to use a service, make sure both the firewall allow the service's packets to go through the ISG50.

Note: The ISG50 checks firewall rules before it checks bandwidth management rules for traffic going through the ISG50.

Bandwidth management examines every TCP and UDP connection passing through the ISG50. Then, you can specify, by port, whether or not the ISG50 continues to route the connection.

DiffServ and DSCP Marking

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is from which zone the connection was initiated and to which zone the connection is going.

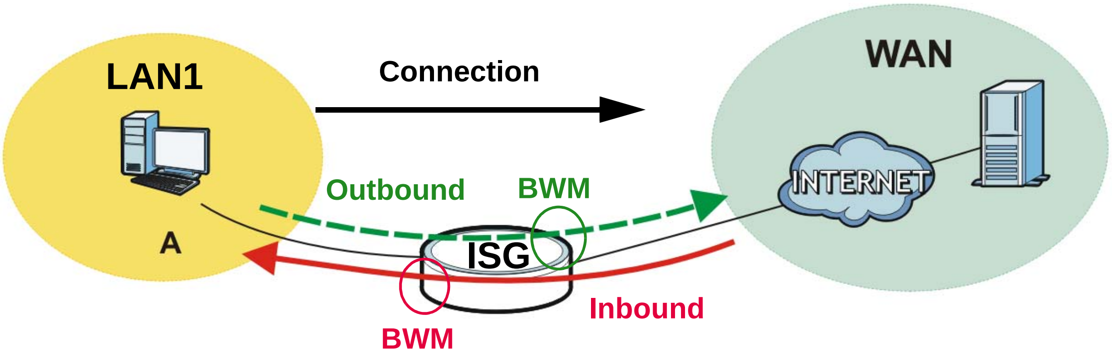
A connection has outbound and inbound packet flows. The ISG50 controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 zone device to a WAN zone device. Bandwidth management is applied before sending the packets out a WAN zone interface on the ISG50.
- Inbound traffic comes back from the WAN zone device to the LAN1 zone device. Bandwidth management is applied before sending the traffic out a LAN1 zone interface.

Figure 259 LAN1 to WAN Connection and Packet Directions



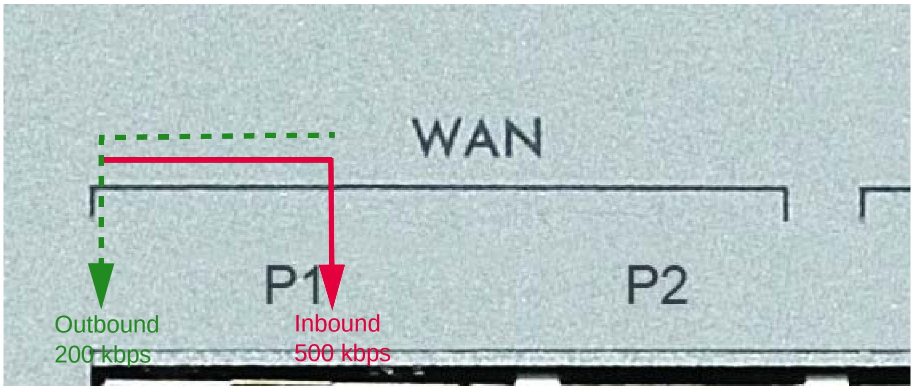
Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.

- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 260 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The ISG50 gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The ISG50 uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The ISG50 automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

After each application gets its configured bandwidth rate, the ISG50 uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

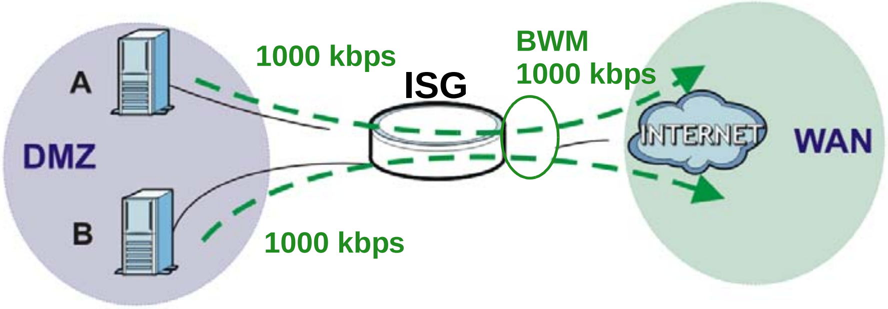
Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers **A** and **B**. Each server tries to send

1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**'s traffic and policy B for server **B**'s traffic.

Figure 261 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 129 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps for server **B**.

Table 130 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the ISG50 divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 131 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the ISG50 still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

Table 132 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

Finding Out More

- See Section 7.5 on page 116 for an example of how to set up web surfing policies with bandwidth restrictions.
- See DSCP Marking and Per-Hop Behavior on page 291 for a description of DSCP marking.

25.1.3 Bandwidth Management Examples

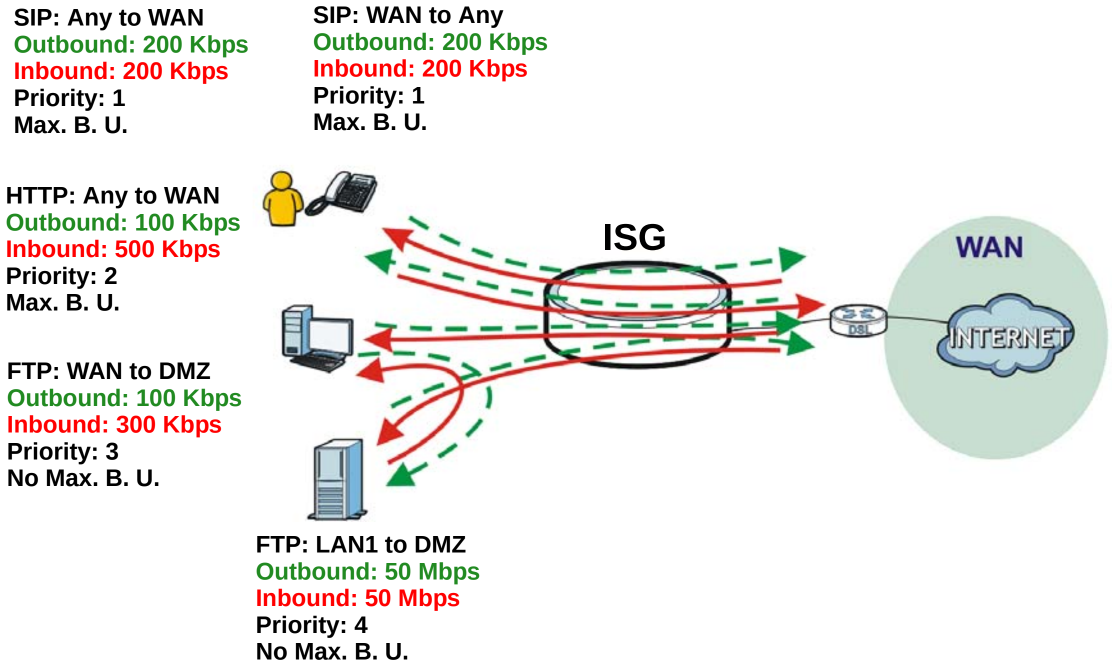
Bandwidth management is very useful when applications are competing for limited bandwidth. For example, say you have a WAN zone interface connected to an ADSL device with a 8 Mbps downstream and 1 Mbps upstream ADSL connection.

Here is an overview of what the rules need to accomplish. See the following sections for more details.

- SIP traffic from VIP users must get through with the least possible delay regardless of if it is an outgoing call or an incoming call. The VIP users must be able to make and receive SIP calls no matter which interface they are connected to.
- HTTP traffic needs to be given priority over FTP traffic.
- FTP traffic from the WAN to the DMZ must be limited so it does not interfere with SIP and HTTP traffic.

- FTP traffic from the LAN1 to the DMZ can use more bandwidth since the interfaces support up to 1 Gbps connections, but it must be the lowest priority and limited so it does not interfere with SIP and HTTP traffic.

Figure 262 Bandwidth Management Example


SIP: Any to WAN
Outbound: 200 Kbps
Inbound: 200 Kbps
Priority: 1
Max. B. U.
SIP: WAN to Any
Outbound: 200 Kbps
Inbound: 200 Kbps
Priority: 1
Max. B. U.
HTTP: Any to WAN
Outbound: 100 Kbps
Inbound: 500 Kbps
Priority: 2
Max. B. U.
ISG
WAN
DSL
INTERNET
FTP: WAN to DMZ
Outbound: 100 Kbps
Inbound: 300 Kbps
Priority: 3
No Max. B. U.
FTP: LAN1 to DMZ
Outbound: 50 Mbps
Inbound: 50 Mbps
Priority: 4
No Max. B. U.

25.1.3.1 Setting the Interface's Bandwidth

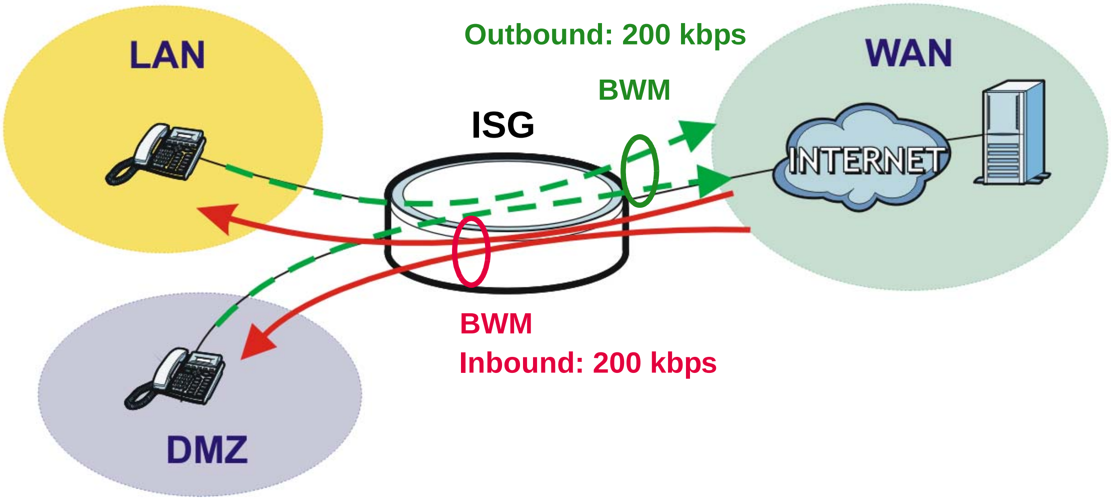
Use the interface screens to set the WAN zone interface's upstream bandwidth to be equal to (or slightly less than) what the connected device can support. This example uses 1000 Kbps.

25.1.3.2 SIP Any to WAN Bandwidth Management Example

- Manage SIP traffic going to the WAN zone from a VIP user on the LAN or DMZ.
- Outbound traffic (to the WAN from the LAN and DMZ) is limited to 200 kbps. The ISG50 applies this limit before sending the traffic to the WAN.
- Inbound traffic (to the LAN and DMZ from the WAN) is also limited to 200 kbps. The ISG50 applies this limit before sending the traffic to LAN or DMZ.

- Enable maximize bandwidth usage so the SIP traffic can borrow unused bandwidth.

Figure 263 SIP Any to WAN Bandwidth Management Example


Outbound: 200 kbps
LAN
WAN
BWM
ISG
INTERNET
BWM
Inbound: 200 kbps
DMZ

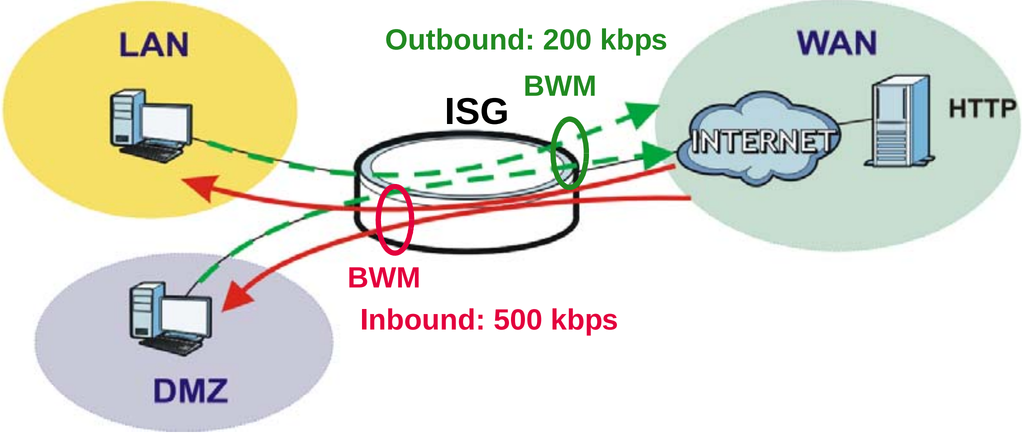
25.1.3.3 SIP WAN to Any Bandwidth Management Example

You also create a policy for calls coming in from the SIP server on the WAN. It is the same as the SIP Any to WAN policy, but with the directions reversed (WAN to Any instead of Any to WAN).

25.1.3.4 HTTP Any to WAN Bandwidth Management Example

- Inbound traffic gets more bandwidth as the local users will probably download more than they upload (and the ADSL connection supports this).
- Second highest priority (2). Set policies for other applications (except SIP) to lower priorities so the local users' HTTP traffic gets sent before non-SIP traffic.
- Enable maximize bandwidth usage so the HTTP traffic can borrow unused bandwidth.

Figure 264 HTTP Any to WAN Bandwidth Management Example

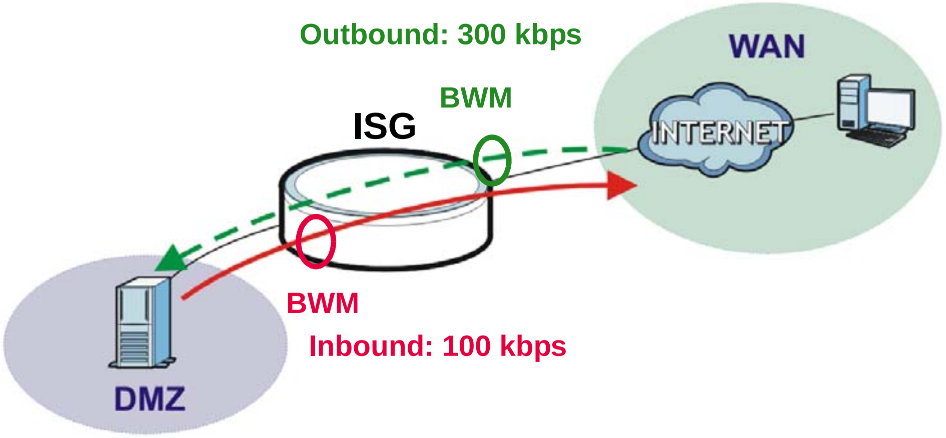

LAN
Outbound: 200 kbps
WAN
BWM
ISG
INTERNET
HTTP
BWM
Inbound: 500 kbps
DMZ

25.1.3.5 FTP WAN to DMZ Bandwidth Management Example

- ADSL supports more downstream than upstream so you allow remote users 300 kbps for uploads to the DMZ FTP server (outbound) but only 100 kbps for downloads (inbound).
- Third highest priority (3).

- Disable maximize bandwidth usage since you do not want to give FTP more bandwidth.

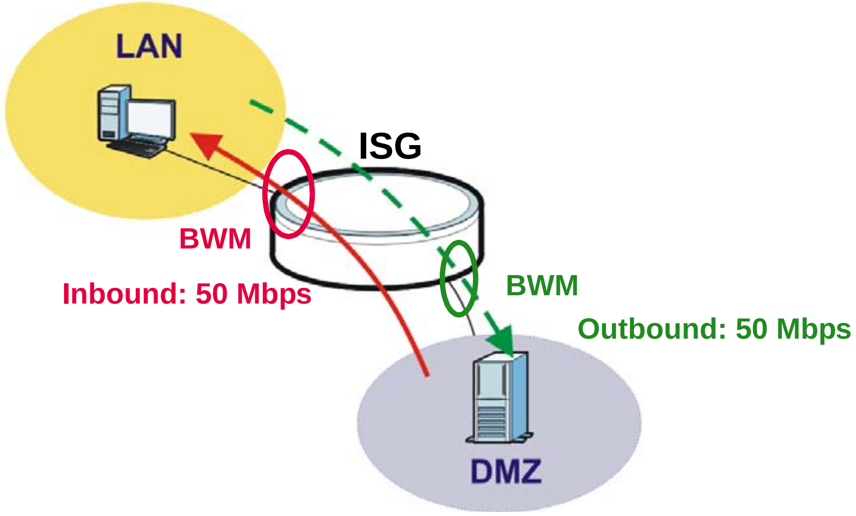
Figure 265 FTP WAN to DMZ Bandwidth Management Example



25.1.3.6 FTP LAN to DMZ Bandwidth Management Example

- The LAN and DMZ zone interfaces are connected to Ethernet networks (not an ADSL device) so you limit both outbound and inbound traffic to 50 Mbps.
- Fourth highest priority (4).
- Disable maximize bandwidth usage since you do not want to give FTP more bandwidth.

Figure 266 FTP LAN to DMZ Bandwidth Management Example

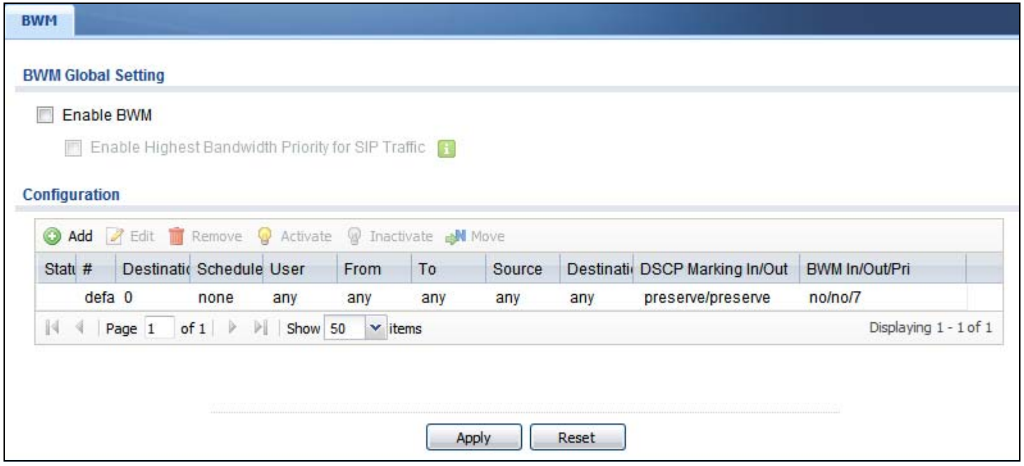


25.2 The Bandwidth Management Screen

The Bandwidth management screen controls the default policy for TCP and UDP traffic. You can use source zone, destination zone, destination port, schedule, user, source, and destination information as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify what the ISG50 should do more precisely.This screen also allows you to add, edit, and remove conditions to this default policy.

Click **Configuration > Bandwidth Management** to open the following screen.

Figure 267 Configuration > Bandwidth Management



☐ Enable BWM

☐ Enable Highest Bandwidth Priority for SIP Traffic

Statu	#	Destinati	Schedule	User	From	To	Source	Destinati	DSCP Marking In/Out	BWM In/Out/Pri
	defa	0	none	any	any	any	any	any	preserve/preserve	no/no/7

The following table describes the labels in this screen. See Section 25.2.1 on page 406 for more information as well.

Table 133 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Enable BWM	Select this check box to activate management bandwidth.
Enable Highest Bandwidth Priority for SIP Traffic	Select this to maximize the throughput of SIP traffic to improve SIP-based VoIP call sound quality. This has the ISG50 immediately send SIP traffic upon identifying it. When this option is enabled the ISG50 ignores any other bandwidth management rules for SIP traffic (so there is no bandwidth control for SIP traffic) and does not record SIP traffic bandwidth usage statistics.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change an entry’s position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This field is a sequential value, and it is not associated with a specific condition. Note: The ISG50 checks conditions in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the ISG50 by putting more common conditions at the top of the list.
Destination Port	This field displays the specific port number to which this policy applies.
Schedule	This is the schedule that defines when the policy applies. **any** means the policy always applies.
User	This is the user name or user group to which the policy applies. If **any** displays, the policy applies to all users.
From	This is the source zone of the traffic to which this policy applies.

Table 133 Configuration > Bandwidth Management

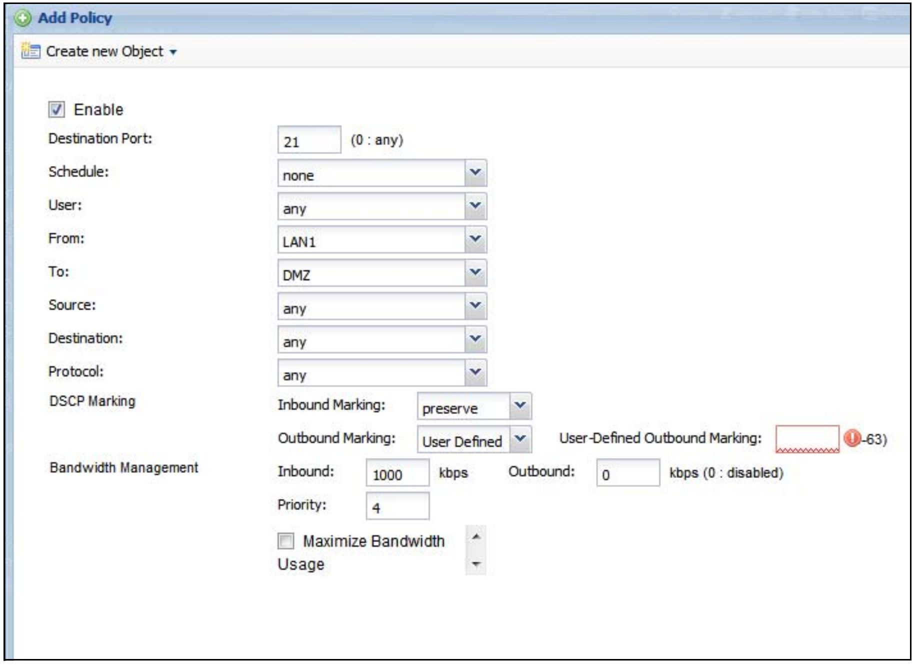
LABEL	DESCRIPTION
To	This is the destination zone of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If **any** displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If **any** displays, the policy is effective for every destination.
DSCP Marking	This is how the ISG50 handles the DSCP value of the outgoing packets that match this policy. **In** - Inbound, the traffic the ISG50 sends to a connection's initiator. **Out** - Outbound, the traffic the ISG50 sends out from a connection's initiator. If this field displays a DSCP value, the ISG50 applies that DSCP value to the route's outgoing packets. **preserve** means the ISG50 does not modify the DSCP value of the route's outgoing packets. **default** means the ISG50 sets the DSCP value of the route's outgoing packets to 0. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 299 for more details.
BWM	These fields show the amount of bandwidth the traffic can use. **In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the ISG50 sends to a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the inbound traffic. **Out** - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the ISG50 sends out from a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the outbound traffic. **Pri** - This is the priority for the traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ISG50 ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

25.2.1 The Bandwidth Management Add/Edit Screen

The **Configuration > Bandwidth Management Add/Edit** screen allows you to create a new condition or edit an existing one. To access this screen, go to the **Configuration > Bandwidth**

Management screen (see Section 25.2 on page 404), and click either the **Add** icon or an **Edit** icon.

Figure 268 Configuration > Bandwidth Management > Edit



☑ Enable
Destination Port: 21 (0 : any)
Schedule: none
User: any
From: LAN1
To: DMZ
Source: any
Destination: any
Protocol: any
DSCP Marking
Inbound Marking: preserve
Outbound Marking: User Defined
User-Defined Outbound Marking: (0-63)
Bandwidth Management
Inbound: 1000 kbps
Outbound: 0 kbps (0 : disabled)
Priority: 4
☐ Maximize Bandwidth Usage

The following table describes the labels in this screen.

Table 134 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to turn on this policy.
Destination Port	Use this field to specify a specific port number to which to apply this policy. Type zero, if this policy applies for every port number.
Schedule	Select a schedule that defines when the policy applies or select **Create Object** to configure a new one (see Chapter 47 on page 625 for details). Otherwise, select **any** to make the policy always effective.
User	Select a user name or user group to which to apply the policy. Use **Create new Object** if you need to configure a new user account (see Section 44.2.1 on page 602 for details). Select **any** to apply the policy for every user.
From	Select the source zone of the traffic to which this policy applies.
To	Select the destination zone of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Use **Create new Object** if you need to configure a new one. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group for whom this policy applies. Use **Create new Object** if you need to configure a new one. Select **any** if the policy is effective for every destination.
Protocol	Select the protocol for which this condition applies. Choices are: **TCP** and **UDP**. Select **any** to apply the policy to both TCP and UDP traffic.

Table 134 Configuration > Bandwidth Management

LABEL	DESCRIPTION
DSCP Marking	Set how the ISG50 handles the DSCP value of the outgoing packets that match this policy. Inbound refers to the traffic the ISG50 sends to a connection's initiator. Outbound refers to the traffic the ISG50 sends out from a connection's initiator. Select one of the pre-defined DSCP values to apply or select **User Defined** to specify another DSCP value. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 299 for more details. Select **preserve** to have the ISG50 keep the packets' original DSCP value. Select **default** to have the ISG50 set the DSCP value of the packets to 0.
Bandwidth Management	Configure these fields to set the amount of bandwidth the application can use.
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the ISG50 sends to a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ISG50 sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the ISG50 sends out from a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ISG50 sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Priority	This field displays when the inbound or outbound bandwidth management is not set to 0. Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ISG50 uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Maximize Bandwidth Usage	This field displays when the inbound or outbound bandwidth management is not set to 0. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface. After each application or type of traffic gets its configured bandwidth rate, the ISG50 uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.

Table 134 Configuration > Bandwidth Management

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

26

ADP

26.1 Overview

This chapter introduces ADP (Anomaly Detection and Prevention), anomaly profiles and applying an ADP profile to a traffic direction. ADP protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans.

26.1.1 ADP

1. ADP anomaly detection is in general effective against abnormal behavior.
2. ADP traffic and anomaly rules are updated when you upload new firmware.

26.1.2 What You Can Do in this Chapter

- Use **Anti-X > ADP > General** (Section 26.2 on page 412) to turn anomaly detection on or off and apply anomaly profiles to traffic directions.
- Use **Anti-X > ADP > Profile** (Section 26.3 on page 413) to add a new profile, edit an existing profile or delete an existing profile.

26.1.3 What You Need To Know

Traffic Anomalies

Traffic anomaly rules look for abnormal behavior or events such as port scanning, sweeping or network flooding. It operates at OSI layer-2 and layer-3. Traffic anomaly rules may be updated when you upload new firmware.

Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder. Protocol anomaly rules may be updated when you upload new firmware.

ADP Profile

An ADP profile is a set of traffic anomaly rules and protocol anomaly rules that you can activate as a set and configure common log and action settings. You can apply ADP profiles to traffic flowing from one zone to another.

Base ADP Profiles

Base ADP profiles are templates that you use to create new ADP profiles.The ISG50 comes with several base profiles. See Table 136 on page 414 for details on ADP base profiles.

ADP Policy

An ADP policy refers to application of an ADP profile to a traffic flow.

Finding Out More

- See Section 6.6.16 on page 103 for ADP prerequisites.
- See Section 26.4 on page 421 for background information on these screens.

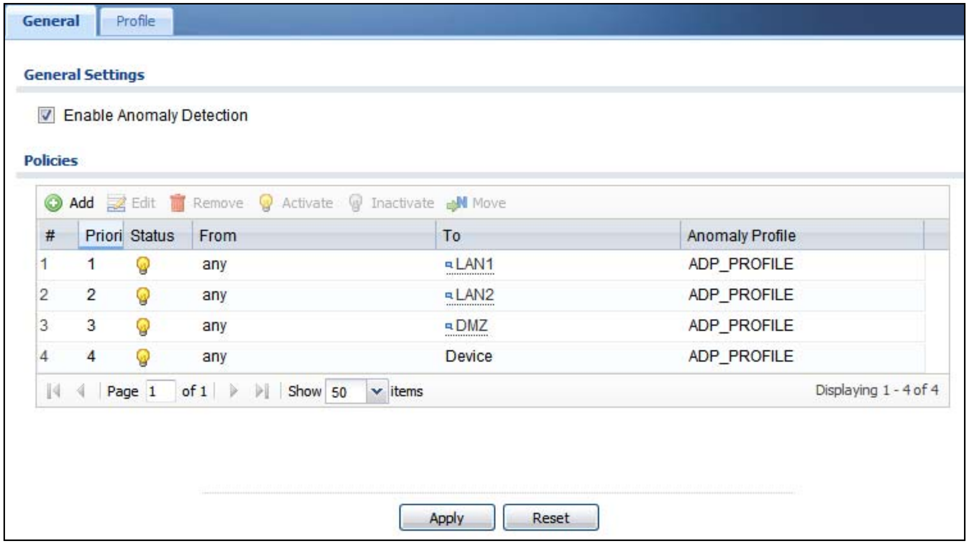
26.1.4 Before You Begin

Configure the ISG50's zones - see Chapter 16 on page 313 for more information.

26.2 The ADP General Screen

Click **Configuration > Anti-X > ADP > General**. Use this screen to turn anomaly detection on or off and apply anomaly profiles to traffic directions.

Figure 269 Configuration > Anti-X > ADP > General


General
Profile
General Settings
Policies
Add
Edit
Remove
Activate
Inactivate
Move
Page 1 of 1
Show 50 items
Displaying 1 - 4 of 4
Apply
Reset

☑ Enable Anomaly Detection

#	Priori	Status	From	To	Anomaly Profile
1	1	💡	any	LAN1	ADP_PROFILE
2	2	💡	any	LAN2	ADP_PROFILE
3	3	💡	any	DMZ	ADP_PROFILE
4	4	💡	any	Device	ADP_PROFILE

The following table describes the screens in this screen.

Table 135 Configuration > Anti-X > ADP > General

LABEL	DESCRIPTION
General Settings	
Enable Anomaly Detection	Select this check box to enable traffic anomaly and protocol anomaly detection.

Table 135 Configuration > Anti-X > ADP > General (continued)

LABEL	DESCRIPTION
Policies	Use this list to specify which anomaly profile the ISG50 uses for traffic flowing in a specific direction. Edit the policies directly in the table.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This is the entry's index number in the list.
Priority	This is the rank in the list of anomaly profile policies. The list is applied in order of priority.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
From, To	This is the direction of travel of packets to which an anomaly profile is bound. Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to. Use the **From** field to specify the zone from which the traffic is coming. Select **ISG50** to specify traffic coming from the ISG50 itself. Use the **To** field to specify the zone to which the traffic is going. Select **ISG50** to specify traffic destined for the ISG50 itself. **From LAN1 To LAN1** means packets traveling from a computer on one LAN1 subnet to a computer on another LAN1 subnet via the ISG50's LAN1 zone interfaces. The ISG50 does not check packets traveling from a LAN1 computer to another LAN1 computer on the same subnet. **From WAN To WAN** means packets that come in from the WAN zone and the ISG50 routes back out through the WAN zone. Note: Depending on your network topology and traffic load, applying every packet direction to an anomaly profile may affect the ISG50's performance.
Anomaly Profile	An anomaly profile is a set of anomaly rules with configured activation, log and action settings. This field shows which anomaly profile is bound to which traffic direction. Select an ADP profile to apply to the entry's traffic direction. Configure the ADP profiles in the ADP profile screens.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

26.3 The Profile Summary Screen

Use this screen to:

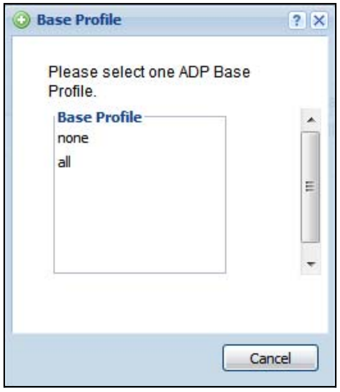
- Create a new profile using an existing base profile
- Edit an existing profile

- Delete an existing profile

26.3.1 Base Profiles

The ISG50 comes with base profiles. You use base profiles to create new profiles. In the **Configuration > Anti-X > ADP > Profile** screen, click **Add** to display the following screen.

Figure 270 Base Profiles


Base Profile
Base Profile
none
all
Cancel

Please select one ADP Base Profile.

These are the default base profiles at the time of writing.

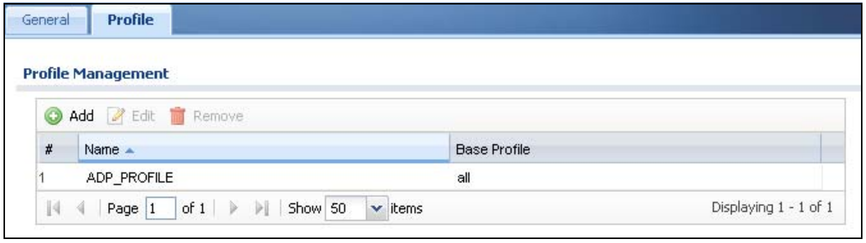
Table 136 Base Profiles

BASE PROFILE	DESCRIPTION
none	All traffic anomaly and protocol anomaly rules are disabled. No logs are generated nor actions are taken.
all	All traffic anomaly and protocol anomaly rules are enabled. Rules with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Rules with a very low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

26.3.2 Configuring The ADP Profile Summary Screen

Select **Configuration > Anti-X > ADP > Profile**.

Figure 271 Configuration > Anti-X > ADP > Profile


General
Profile
Profile Management
Add
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1

#	Name	Base Profile
1	ADP_PROFILE	all

The following table describes the fields in this screen.

Table 137 Anti-X > ADP > Profile

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This is the entry's index number in the list.
Name	This is the name of the profile you created.
Base Profile	This is the base profile from which the profile was created.

26.3.3 Creating New ADP Profiles

You may want to create a new profile if not all rules in a base profile are applicable to your network. In this case you should disable non-applicable rules so as to improve ISG50 ADP processing efficiency.

You may also find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ISG50. As each network is different, false positives and false negatives are common on initial ADP deployment.

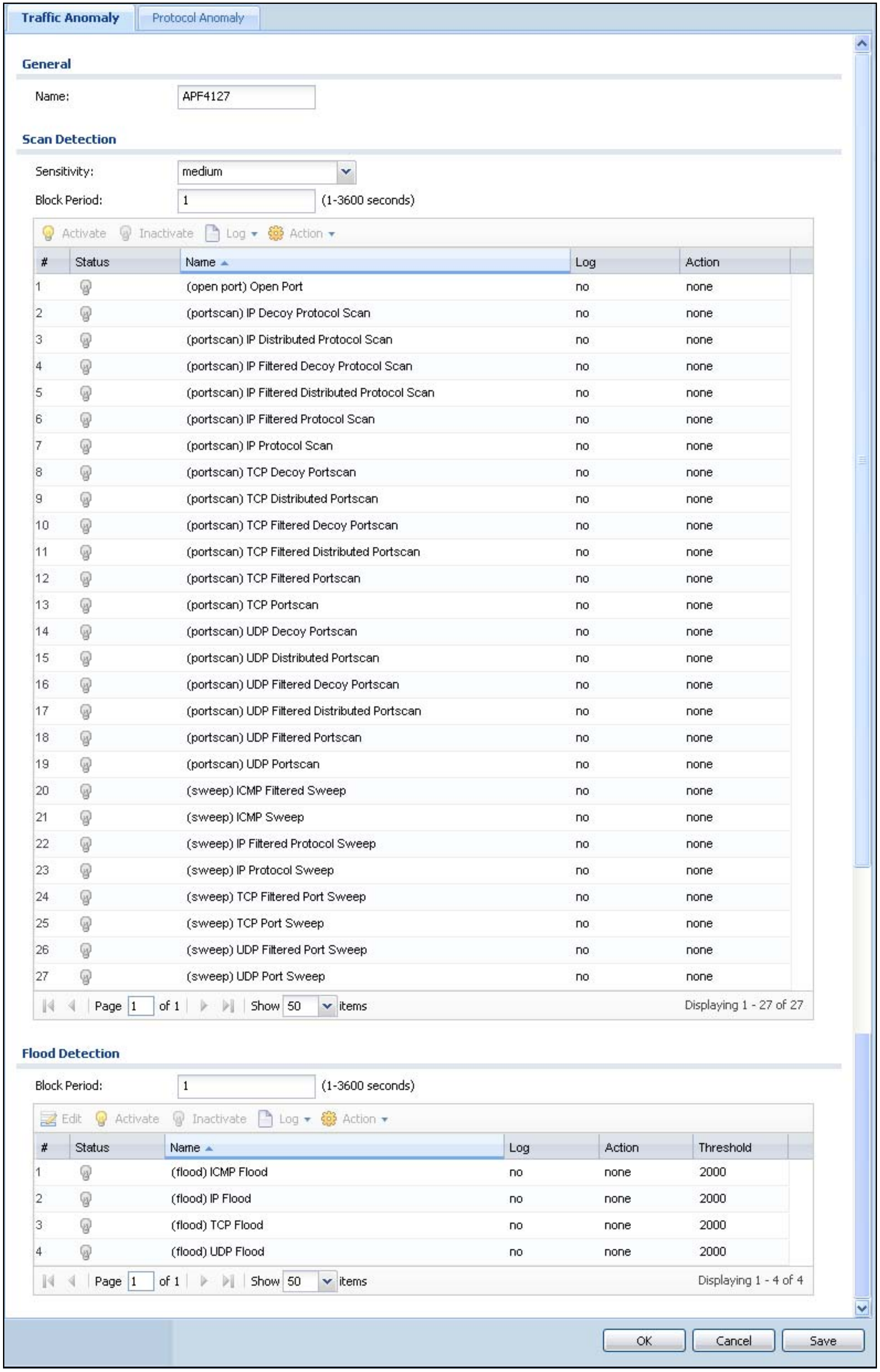
You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a rule.

ADP profiles consist of traffic anomaly profiles and protocol anomaly profiles. To create a new profile, select a base profile (see Table 136 on page 414) and then click **OK** to go to the profile details screen. Type a new profile name, enable or disable individual rules and then edit the default log options and actions.

26.3.4 Traffic Anomaly Profiles

The traffic anomaly screen is the second screen in an ADP profile. Traffic anomaly detection looks for abnormal behavior such as scan or flooding attempts. In the **Configuration > Anti-X > ADP > Profile** screen, click the **Edit** icon or click the **Add** icon and choose a base profile. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Traffic Anomaly** tab.

Figure 272 Profiles: Traffic Anomaly



General

Name: APF4127

Scan Detection

Sensitivity: medium

Block Period: 1 (1-3600 seconds)

#	Status	Name	Log	Action
1		(open port) Open Port	no	none
2		(portscan) IP Decoy Protocol Scan	no	none
3		(portscan) IP Distributed Protocol Scan	no	none
4		(portscan) IP Filtered Decoy Protocol Scan	no	none
5		(portscan) IP Filtered Distributed Protocol Scan	no	none
6		(portscan) IP Filtered Protocol Scan	no	none
7		(portscan) IP Protocol Scan	no	none
8		(portscan) TCP Decoy Portscan	no	none
9		(portscan) TCP Distributed Portscan	no	none
10		(portscan) TCP Filtered Decoy Portscan	no	none
11		(portscan) TCP Filtered Distributed Portscan	no	none
12		(portscan) TCP Filtered Portscan	no	none
13		(portscan) TCP Portscan	no	none
14		(portscan) UDP Decoy Portscan	no	none
15		(portscan) UDP Distributed Portscan	no	none
16		(portscan) UDP Filtered Decoy Portscan	no	none
17		(portscan) UDP Filtered Distributed Portscan	no	none
18		(portscan) UDP Filtered Portscan	no	none
19		(portscan) UDP Portscan	no	none
20		(sweep) ICMP Filtered Sweep	no	none
21		(sweep) ICMP Sweep	no	none
22		(sweep) IP Filtered Protocol Sweep	no	none
23		(sweep) IP Protocol Sweep	no	none
24		(sweep) TCP Filtered Port Sweep	no	none
25		(sweep) TCP Port Sweep	no	none
26		(sweep) UDP Filtered Port Sweep	no	none
27		(sweep) UDP Port Sweep	no	none

Page 1 of 1 | Show 50 items | Displaying 1 - 27 of 27

Flood Detection

Block Period: 1 (1-3600 seconds)

#	Status	Name	Log	Action	Threshold
1		(flood) ICMP Flood	no	none	2000
2		(flood) IP Flood	no	none	2000
3		(flood) TCP Flood	no	none	2000
4		(flood) UDP Flood	no	none	2000

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

The following table describes the fields in this screen.

Table 138 Configuration > ADP > Profile > Traffic Anomaly

LABEL	DESCRIPTION
Name	This is the name of the ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: MyProfile mYProfile Mymy12_3-4 These are invalid profile names: 1mYProfile My Profile MyProfile? Whatalongprofilename123456789012
Scan/Flood Detection	
Sensitivity	(Scan detection only.) Select a sensitivity level so as to reduce false positives in your network. If you choose low sensitivity, then scan thresholds and sample times are set low, so you will have fewer logs and false positives; however some traffic anomaly attacks may not be detected. If you choose high sensitivity, then scan thresholds and sample times are set high, so most traffic anomaly attacks will be detected; however you will have more logs and false positives.
Block Period	Specify for how many seconds the ISG50 blocks all packets from being sent to the victim (destination) of a detected anomaly attack.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Log	To edit an item's log option, select it and use the **Log** icon. Select whether to have the ISG50 generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 53 on page 705 for more on logs.
Action	To edit what action the ISG50 takes when a packet matches a rule, select the signature and use the **Action** icon. **none**: The ISG50 takes no action when a packet matches the signature(s). **block**: The ISG50 silently drops packets that matches the rule. Neither sender nor receiver are notified.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the traffic anomaly rule. Click the **Name** column heading to sort in ascending or descending order according to the rule name.
Log	These are the log options. To edit this, select an item and use the **Log** icon.
Action	This is the action the ISG50 should take when a packet matches a rule. To edit this, select an item and use the **Action** icon.
Threshold	For flood detection you can set the number of detected flood packets per second that causes the ISG50 to take the configured action.
OK	Click **OK** to save your settings to the ISG50, complete the profile and return to the profile summary page.

Table 138 Configuration > ADP > Profile > Traffic Anomaly (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the ISG50 but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

26.3.5 Protocol Anomaly Profiles

Protocol anomaly is the third screen in an ADP profile. Protocol anomaly (PA) rules check for protocol compliance against the relevant RFC (Request for Comments).

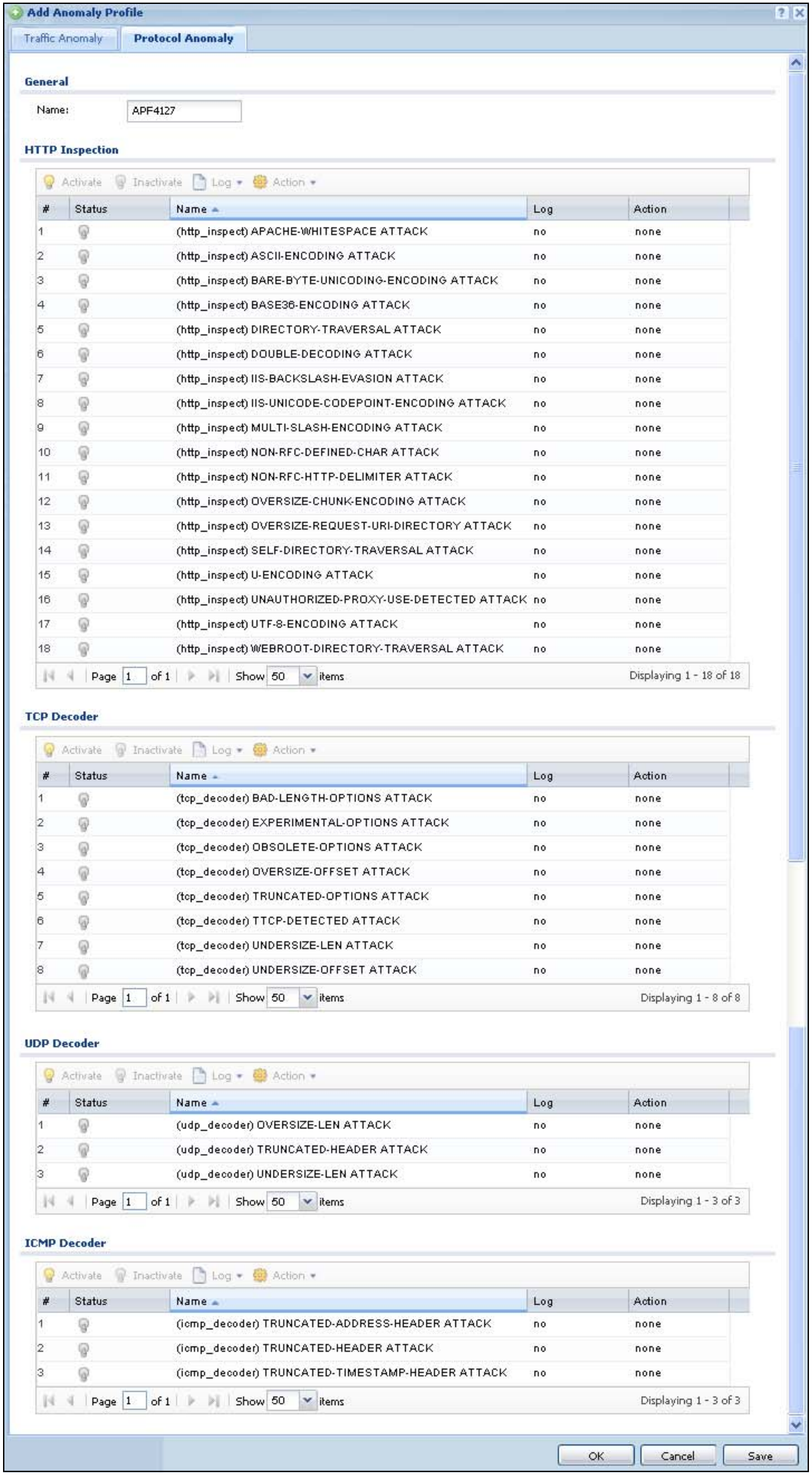
Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder, and ICMP Decoder where each category reflects the packet type inspected.

Protocol anomaly rules may be updated when you upload new firmware.

26.3.6 Protocol Anomaly Configuration

In the **Configuration > Anti-X > ADP > Profile** screen, click the **Edit** icon or click the **Add** icon and choose a base profile, then select the **Protocol Anomaly** tab. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Protocol Anomaly** tab.

Figure 273 Profiles: Protocol Anomaly



General

Name: APF4127

HTTP Inspection

#	Status	Name	Log	Action
1		(http_inspect) APACHE-WHITESPACE ATTACK	no	none
2		(http_inspect) ASCII-ENCODING ATTACK	no	none
3		(http_inspect) BARE-BYTE-UNICODING-ENCODING ATTACK	no	none
4		(http_inspect) BASE36-ENCODING ATTACK	no	none
5		(http_inspect) DIRECTORY-TRAVERSAL ATTACK	no	none
6		(http_inspect) DOUBLE-DECODING ATTACK	no	none
7		(http_inspect) IIS-BACKSLASH-EVASION ATTACK	no	none
8		(http_inspect) IIS-UNICODE-CODEPOINT-ENCODING ATTACK	no	none
9		(http_inspect) MULTI-SLASH-ENCODING ATTACK	no	none
10		(http_inspect) NON-RFC-DEFINED-CHAR ATTACK	no	none
11		(http_inspect) NON-RFC-HTTP-DELIMITER ATTACK	no	none
12		(http_inspect) OVERSIZE-CHUNK-ENCODING ATTACK	no	none
13		(http_inspect) OVERSIZE-REQUEST-URI-DIRECTORY ATTACK	no	none
14		(http_inspect) SELF-DIRECTORY-TRAVERSAL ATTACK	no	none
15		(http_inspect) U-ENCODING ATTACK	no	none
16		(http_inspect) UNAUTHORIZED-PROXY-USE-DETECTED ATTACK	no	none
17		(http_inspect) UTF-8-ENCODING ATTACK	no	none
18		(http_inspect) WEBROOT-DIRECTORY-TRAVERSAL ATTACK	no	none

Page 1 of 1 | Show 50 items | Displaying 1 - 18 of 18

TCP Decoder

#	Status	Name	Log	Action
1		(tcp_decoder) BAD-LENGTH-OPTIONS ATTACK	no	none
2		(tcp_decoder) EXPERIMENTAL-OPTIONS ATTACK	no	none
3		(tcp_decoder) OBSOLETE-OPTIONS ATTACK	no	none
4		(tcp_decoder) OVERSIZE-OFFSET ATTACK	no	none
5		(tcp_decoder) TRUNCATED-OPTIONS ATTACK	no	none
6		(tcp_decoder) TTCP-DETECTED ATTACK	no	none
7		(tcp_decoder) UNDERSIZE-LEN ATTACK	no	none
8		(tcp_decoder) UNDERSIZE-OFFSET ATTACK	no	none

Page 1 of 1 | Show 50 items | Displaying 1 - 8 of 8

UDP Decoder

#	Status	Name	Log	Action
1		(udp_decoder) OVERSIZE-LEN ATTACK	no	none
2		(udp_decoder) TRUNCATED-HEADER ATTACK	no	none
3		(udp_decoder) UNDERSIZE-LEN ATTACK	no	none

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

ICMP Decoder

#	Status	Name	Log	Action
1		(icmp_decoder) TRUNCATED-ADDRESS-HEADER ATTACK	no	none
2		(icmp_decoder) TRUNCATED-HEADER ATTACK	no	none
3		(icmp_decoder) TRUNCATED-TIMESTAMP-HEADER ATTACK	no	none

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

The following table describes the fields in this screen.

Table 139 Configuration > ADP > Profile > Protocol Anomaly

LABEL	DESCRIPTION
Name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: MyProfile mYProfile Mymy12_3-4 These are invalid profile names: 1mYProfile My Profile MyProfile? Whatalongprofilename123456789012
HTTP Inspection/TCP Decoder/UDP Decoder/ICMP Decoder	
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Log	To edit an item's log option, select it and use the **Log** icon. Select whether to have the ISG50 generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 53 on page 705 for more on logs.
Action	To edit what action the ISG50 takes when a packet matches a signature, select the signature and use the **Action** icon. **none**: Select this action on an individual signature or a complete service group to have the ISG50 take no action when a packet matches a rule. **drop**: Select this action on an individual signature or a complete service group to have the ISG50 silently drop a packet that matches a rule. Neither sender nor receiver are notified. **reject-sender**: Select this action on an individual signature or a complete service group to have the ISG50 send a reset to the sender when a packet matches the signature. If it is a TCP attack packet, the ISG50 will send a packet with a 'RST' flag. If it is an ICMP or UDP attack packet, the ISG50 will send an ICMP unreachable packet. **reject-receiver**: Select this action on an individual signature or a complete service group to have the ISG50 send a reset to the receiver when a packet matches the rule. If it is a TCP attack packet, the ISG50 will send a packet with an a 'RST' flag. If it is an ICMP or UDP attack packet, the ISG50 will do nothing. **reject-both**: Select this action on an individual signature or a complete service group to have the ISG50 send a reset to both the sender and receiver when a packet matches the rule. If it is a TCP attack packet, the ISG50 will send a packet with a 'RST' flag to the receiver and sender. If it is an ICMP or UDP attack packet, the ISG50 will send an ICMP unreachable packet.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the protocol anomaly rule. Click the **Name** column heading to sort in ascending or descending order according to the protocol anomaly rule name.
Activation	Click the icon to enable or disable a rule or group of rules.

Table 139 Configuration > ADP > Profile > Protocol Anomaly (continued)

LABEL	DESCRIPTION
Log	These are the log options. To edit this, select an item and use the **Log** icon.
Action	This is the action the ISG50 should take when a packet matches a rule. To edit this, select an item and use the **Action** icon.
Log	Select whether to have the ISG50 generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 53 on page 705 for more on logs.
Action	Select what the ISG50 should do when a packet matches a rule. **none**: The ISG50 takes no action when a packet matches the signature(s). **block**: The ISG50 silently drops packets that matches the rule. Neither sender nor receiver are notified.
OK	Click **OK** to save your settings to the ISG50, complete the profile and return to the profile summary page.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.
Save	Click **Save** to save the configuration to the ISG50 but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile.

26.4 ADP Technical Reference

This section is divided into traffic anomaly background information and protocol anomaly background information.

Traffic Anomaly Background Information

The following sections may help you configure the traffic anomaly profile screen (Section 26.3.4 on page 415).

Port Scanning

An attacker scans device(s) to determine what types of network protocols or services a device supports. One of the most common port scanning tools in use today is Nmap.

Many connection attempts to different ports (services) may indicate a port scan. These are some port scan types:

- TCP Portscan
- UDP Portscan
- IP Portscan

An IP port scan searches not only for TCP, UDP and ICMP protocols in use by the remote computer, but also additional IP protocols such as EGP (Exterior Gateway Protocol) or IGP (Interior Gateway Protocol). Determining these additional protocols can help reveal if the destination device is a workstation, a printer, or a router.

Decoy Port Scans

Decoy port scans are scans where the attacker has spoofed the source address. These are some decoy scan types:

- TCP Decoy Portscan
- UDP Decoy Portscan
- IP Decoy Portscan

Distributed Port Scans

Distributed port scans are many-to-one port scans. Distributed port scans occur when multiple hosts query one host for open services. This may be used to evade intrusion detection. These are distributed port scan types:

- TCP Distributed Portscan
- UDP Distributed Portscan
- IP Distributed Portscan

Port Sweeps

Many different connection attempts to the same port (service) may indicate a port sweep, that is, they are one-to-many port scans. One host scans a single port on multiple hosts. This may occur when a new exploit comes out and the attacker is looking for a specific service. These are some port sweep types:

- TCP Portsweep
- UDP Portsweep
- IP Portsweep
- ICMP Portsweep

Filtered Port Scans

A filtered port scan may indicate that there were no network errors (ICMP unreachables or TCP RSTs) or responses on closed ports have been suppressed. Active network devices, such as NAT routers, may trigger these alerts if they send out many connection attempts within a very small amount of time. These are some filtered port scan examples.

- TCP Filtered Portscan
- UDP Filtered Portscan
- IP Filtered Portscan
- TCP Filtered Decoy Portscan
- UDP Filtered Decoy Portscan
- IP Filtered Decoy Portscan
- TCP Filtered Portsweep
- UDP Filtered Portsweep
- IP Filtered Portsweep
- ICMP Filtered Portsweep
- TCP Filtered Distributed Portscan
- UDP Filtered Distributed Portscan
- IP Filtered Distributed Portscan

Flood Detection

Flood attacks saturate a network with useless data, use up all available bandwidth, and therefore make communications in the network impossible.

ICMP Flood Attack

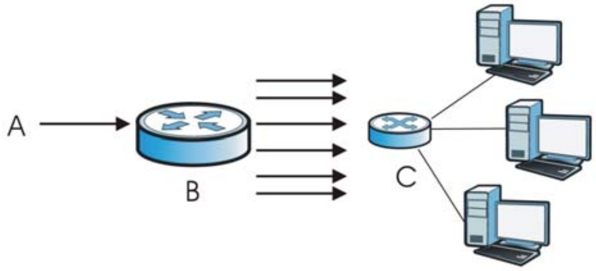
An ICMP flood is broadcasting many pings or UDP packets so that so much data is sent to the system, that it slows it down or locks it up.

Smurf

A smurf attacker (A) floods a router (B) with Internet Control Message Protocol (ICMP) echo request packets (pings) with the destination IP address of each packet as the broadcast address of the network. The router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic.

If an attacker (A) spoofs the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only saturate the receiving network (B), but the network of the spoofed source IP address (C).

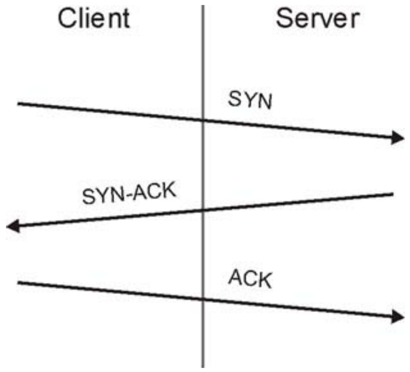
Figure 274 Smurf Attack



TCP SYN Flood Attack

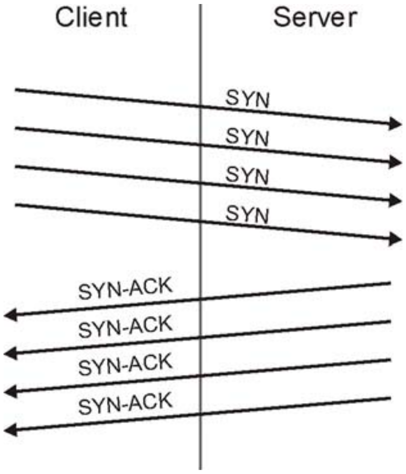
Usually a client starts a session by sending a SYN (synchronize) packet to a server. The receiver returns an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 275 TCP Three-Way Handshake



A SYN flood attack is when an attacker sends a series of SYN packets. Each packet causes the receiver to reply with a SYN-ACK response. The receiver then waits for the ACK that follows the SYN-ACK, and stores all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are only moved off the queue when an ACK comes back or when an internal timer ends the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for other users.

Figure 276 SYN Flood



LAND Attack

In a LAND attack, hackers flood SYN packets into a network with a spoofed source IP address of the network itself. This makes it appear as if the computers in the network sent the packets to themselves, so the network is unavailable while they try to respond to themselves.

UDP Flood Attack

UDP is a connection-less protocol and it does not require any connection setup procedure to transfer data. A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

Protocol Anomaly Background Information

The following sections may help you configure the protocol anomaly profile screen (see Section 26.3.5 on page 418)

HTTP Inspection and TCP/UDP/ICMP Decoders

The following table gives some information on the HTTP inspection, TCP decoder, UDP decoder and ICMP decoder ISG50 protocol anomaly rules.

Table 140 HTTP Inspection and TCP/UDP/ICMP Decoders

LABEL	DESCRIPTION
HTTP Inspection	
APACHE-WHITESPACE ATTACK	This rule deals with non-RFC standard of tab for a space delimiter. Apache uses this, so if you have an Apache server, you need to enable this option.
ASCII-ENCODING ATTACK	This rule can detect attacks where malicious attackers use ASCII-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
BARE-BYTE-UNICODING-ENCODING ATTACK	Bare byte encoding uses non-ASCII characters as valid values in decoding UTF-8 values. This is NOT in the HTTP standard, as all non-ASCII values have to be encoded with a %. Bare byte encoding allows the user to emulate an IIS server and interpret non-standard encodings correctly.
BASE36-ENCODING ATTACK	This is a rule to decode base36-encoded characters. This rule can detect attacks where malicious attackers use base36-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
DIRECTORY-TRAVERSAL ATTACK	This rule normalizes directory traversals and self-referential directories. So, “/abc/this_is_not_a_real_dir/../xyz” get normalized to “/abc/xyz”. Also, “/abc/./xyz” gets normalized to “/abc/xyz”. If a user wants to configure an alert, then specify “yes”, otherwise “no”. This alert may give false positives since some web sites refer to files using directory traversals.
DOUBLE-ENCODING ATTACK	This rule is IIS specific. IIS does two passes through the request URI, doing decodes in each one. In the first pass, IIS encoding (UTF-8 unicode, ASCII, bare byte, and %u) is done. In the second pass ASCII, bare byte, and %u encodings are done.
IIS-BACKSLASH-EVASION ATTACK	This is an IIS emulation rule that normalizes backslashes to slashes. Therefore, a request-URI of “/abc\xyz” gets normalized to “/abc/xyz”.
IIS-UNICODE-CODEPOINT-ENCODING ATTACK	This rule can detect attacks which send attack strings containing non-ASCII characters encoded by IIS Unicode. IIS Unicode encoding references the unicode.map file. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
MULTI-SLASH-ENCODING ATTACK	This rule normalizes multiple slashes in a row, so something like: “abc/////////xyz” get normalized to “abc/xyz”.
NON-RFC-DEFINED-CHAR ATTACK	This rule lets you receive a log or alert if certain non-RFC characters are used in a request URI. For instance, you may want to know if there are NULL bytes in the request-URI.
NON-RFC-HTTP-DELIMITER ATTACK	This is when a newline “\n” character is detected as a delimiter. This is non-standard but is accepted by both Apache and IIS web servers.
OVERSIZE-CHUNK-ENCODING ATTACK	This rule is an anomaly detector for abnormally large chunk sizes. This picks up the apache chunk encoding exploits and may also be triggered on HTTP tunneling that uses chunk encoding.

Table 140 HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

LABEL	DESCRIPTION
OVERSIZE-REQUEST-URI-DIRECTORY ATTACK	This rule takes a non-zero positive integer as an argument. The argument specifies the max character directory length for URL directory. If a URL directory is larger than this argument size, an alert is generated. A good argument value is 300 characters. This should limit the alerts to IDS evasion type attacks, like whisker.
SELF-DIRECTORY-TRAVERSAL ATTACK	This rule normalizes self-referential directories. So, "/abc/./xyz" gets normalized to "/abc/xyz".
U-ENCODING ATTACK	This rule emulates the IIS %u encoding scheme. The %u encoding scheme starts with a %u followed by 4 characters, like %uXXXX. The XXXX is a hex encoded value that correlates to an IIS unicode codepoint. This is an ASCII value. An ASCII character is encoded like, %u002f = /, %u002e = ., etc.
UTF-8-ENCODING ATTACK	The UTF-8 decode rule decodes standard UTF-8 unicode sequences that are in the URI. This abides by the unicode standard and only uses % encoding. Apache uses this standard, so for any Apache servers, make sure you have this option turned on. When this rule is enabled, ASCII decoding is also enabled to enforce correct functioning.
WEBROOT-DIRECTORY-TRAVERSAL ATTACK	This is when a directory traversal traverses past the web server root directory. This generates much fewer false positives than the directory option, because it doesn't alert on directory traversals that stay within the web server directory structure. It only alerts when the directory traversals go past the web server root directory, which is associated with certain web attacks.
TCP Decoder	
BAD-LENGTH-OPTIONS ATTACK	This is when a TCP packet is sent where the TCP option length field is not the same as what it actually is or is 0. This may cause some applications to crash.
EXPERIMENTAL-OPTIONS ATTACK	This is when a TCP packet is sent which contains non-RFC-complaint options. This may cause some applications to crash.
OBSOLETE-OPTIONS ATTACK	This is when a TCP packet is sent which contains obsolete RFC options.
OVERSIZE-OFFSET ATTACK	This is when a TCP packet is sent where the TCP data offset is larger than the payload.
TRUNCATED-OPTIONS ATTACK	This is when a TCP packet is sent which doesn't have enough data to read. This could mean the packet was truncated.
TTCP-DETECTED ATTACK	T/TCP provides a way of bypassing the standard three-way handshake found in TCP, thus speeding up transactions. However, this could lead to unauthorized access to the system by spoofing connections.
UNDERSIZE-LEN ATTACK	This is when a TCP packet is sent which has a TCP datagram length of less than 20 bytes. This may cause some applications to crash.
UNDERSIZE-OFFSET ATTACK	This is when a TCP packet is sent which has a TCP header length of less than 20 bytes.This may cause some applications to crash.
UDP Decoder	
OVERSIZE-LEN ATTACK	This is when a UDP packet is sent which has a UDP length field of greater than the actual packet length. This may cause some applications to crash.
TRUNCATED-HEADER ATTACK	This is when a UDP packet is sent which has a UDP datagram length of less the UDP header length. This may cause some applications to crash.
UNDERSIZE-LEN ATTACK	This is when a UDP packet is sent which has a UDP length field of less than 8 bytes. This may cause some applications to crash.

Table 140 HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

LABEL	DESCRIPTION
ICMP Decoder	
TRUNCATED-ADDRESS-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP address header length. This may cause some applications to crash.
TRUNCATED-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP header length. This may cause some applications to crash.
TRUNCATED-TIMESTAMP-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP Time Stamp header length. This may cause some applications to crash.

27

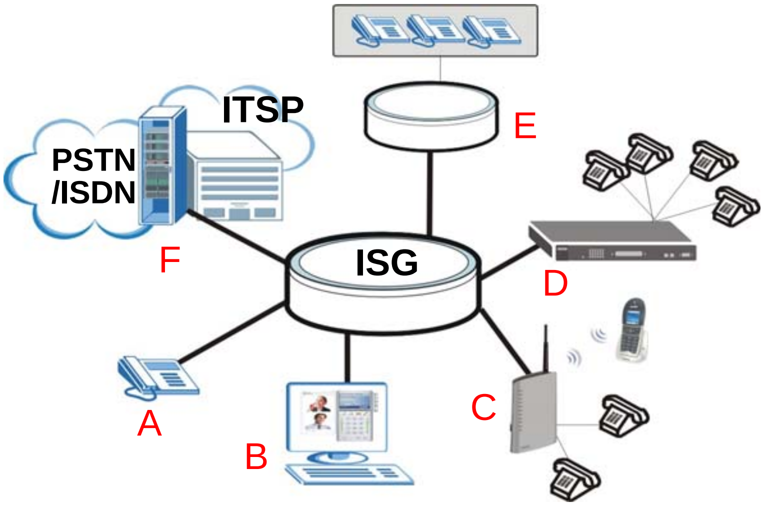
Global PBX Settings

27.1 Overview

This chapter shows you how to set up your ISG50-wide PBX settings including SIP server, feature code, email, fake IP, peer to peer, QoS and TAPI settings.

The following diagram shows SIP devices communicating with the ISG50. In SIP some devices act as clients and others as servers. For example, in the figure below, devices **A**-**D** act as clients and must register with the ISG50 before they are able to make calls via the ISG50. The ISG50 also is a client in relation to the SIP server located at the ITSP (**F**). The ISG50 must register with the ITSP SIP server before calls can be routed to telephones outside its network. Finally, two SIP servers can act as peers, as shown with another ISG50 (**E**) in the figure below. In this case, both ISG50s must register with each other before they can forward each other's calls.

Figure 277 SIP Devices and the ISG50



27.1.1 What You Can Do in this Chapter

- Use the **SIP Server** screen to configure ISG50's general SIP server settings. See Section 27.2 on page 431.
- Use the **Feature Code** screen to configure feature code settings. It allows users to dial a code on their phone's keypad to enable or disable a feature your ISG50 supports. See Section 27.3 on page 433.
- Use the **E-Mail** screen to configure email settings. It allows users to send voice mails or CDR backup data through the email server. See Section 27.4 on page 435.
- Use the **Fake IP** screen to configure settings that may help you to avoid any potential VoIP problems that result from having the ISG50 behind a NAT router. See Section 27.5 on page 435.

- Use the **Peer to peer** screen to set up a direct connection between two IP phones on the same subnet. See Section 27.6 on page 436.
- Use the **QoS** screen to configure Quality of Service (QoS) settings. See Section 27.7 on page 440.
- Use the **TAPI** screen to configure TAPI settings and download the ZyXEL TAPI driver. See Section 27.8 on page 442.

27.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

RTP

When you make a VoIP call using SIP, the RTP (Real Time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

NAT

Network Address Translation (NAT) replaces an IP address used inside one network with a different IP address that is used within another network.

Peer-to-Peer

Peer-to-peer networking has a number of participants whose devices assume the roles of both client and server. Although they are interconnected across existing network lines and hardware, they do not require a central server to manage their data nor do they behave strictly as clients. All participants in a peer-to-peer network can provide data to the others (like a server) while simultaneously receiving data from them (like a client). This type of distributed networking relies on the computing resources of each participant to create and maintain the data swarm. As such, a participant with limited resources can dramatically impact the efficiency of a small peer-to-peer network for the worse; fortunately, as the network grows in size the weakest links are rapidly overshadowed by the bigger, faster participants.

QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as VoIP.

The following problems can occur on a congested network with poor QoS settings:

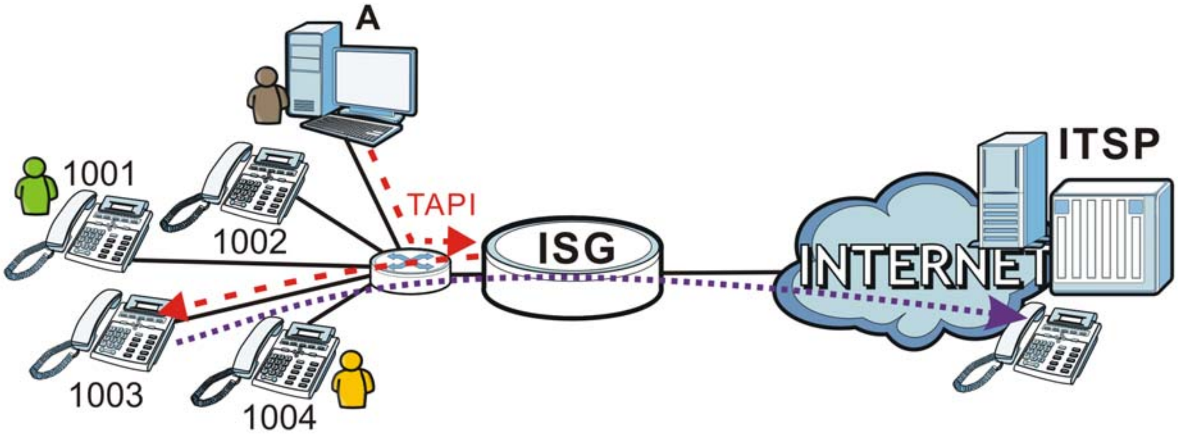
- **Latency** - delay of packet delivery. This can cause echoes during a conversation.
- **Jitter** - variations in delay of packet delivery. This could cause strange sound effects. The ISG50 utilizes a jitter buffer to minimize the effects of jitter.
- **Packet Loss** - packets are dropped due to an overwhelming amount of traffic on the network. Some degree of packet loss will not be noticeable to the end user, but as packet loss increases the quality of sound degrades.

The ISG50 can be configured to change the priority field of IP packets for all outgoing RTP (Real Time Protocol) packets. The ISG50 supports Differentiated Services (DiffServ) for implementing QoS. Configure the ISG50 with the QoS settings that your network uses for VoIP.

TAPI

Microsoft Windows Telephony Application Programming Interface (TAPI) integrates the ISG50's telephone services with user computers. With the TAPI driver installed, you can work as a telephone operator to manage and monitor the extension(s) and/or make a scheduled call from your computer by using the CTI (Computer Telephony Integration) client or server software. The phone services vary by the software you use. A CTI client is the software that can control a phone attached to the ISG50.

In the following example, you installed the ZyXEL TAPI driver and UC server software on computer **A**. After a TAPI connection for extension **1003** is set up between computer **A** and the ISG50, the computer can have extension **1003** make a VoIP call to a specific number at the scheduled time.



You can download the ZyXEL's TAPI driver for the ISG50 from the administrator Web Configurator screen. The TAPI driver can be in either server or client mode. A TAPI server that logs in using the TAPI utility with the pre-defined server account information can control multiple SIP and FXS extensions on the ISG50. A TAPI client that logs in using the TAPI utility with the authentication information for a pre-configured extension can control that extension only.

ZyXEL's TAPI driver also allows you to use Microsoft Outlook from a Windows 2000 or later computer to issue an invite to any person in your address book. When the invite is sent out, the ISG50 rings both your extension and the extension of the invited person. For a snom phone, you can also click to answer a call.

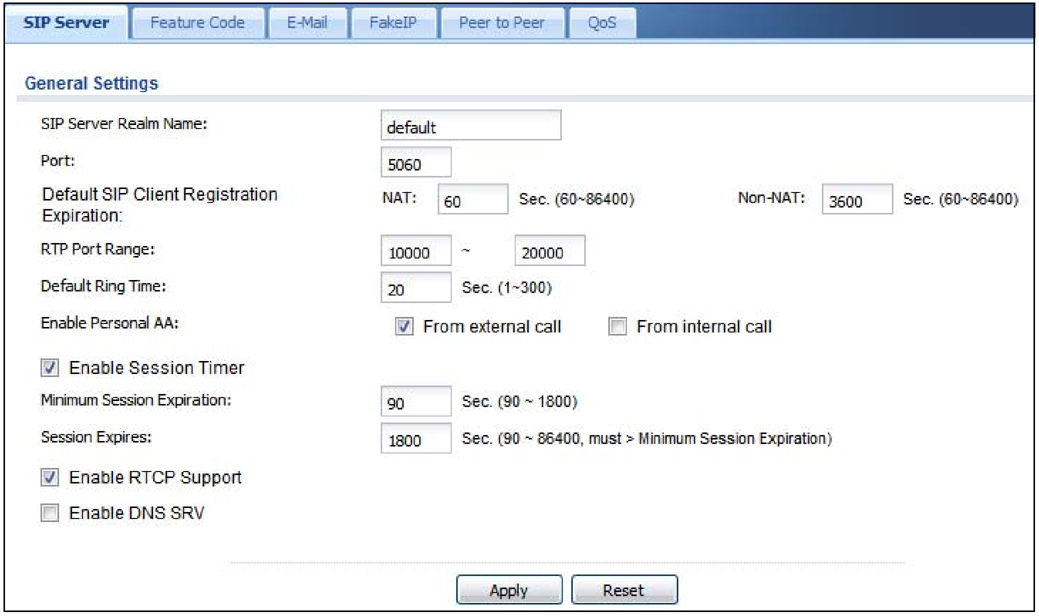
The call features supported by the ZyXEL TAPI driver are making calls, rejecting calls, dropping calls, blind transfer, consult transfer, call pickup, presence and call redirect.

27.2 The SIP Server Screen

Use this screen to set up the SIP server settings on the ISG50. SIP clients, such as the IP phones on your network, must enter this information when registering with the ISG50. To access this screen, click **Configuration > PBX > Global > SIP Server**.

See Section 13.2 on page 285 to set the WAN trunk the ISG50 uses for default traffic.

Figure 278 Configuration > PBX > Global > SIP Server



General Settings

SIP Server Realm Name: default

Port: 5060

Default SIP Client Registration Expiration: NAT: 60 Sec. (60~86400) Non-NAT: 3600 Sec. (60~86400)

RTP Port Range: 10000 ~ 20000

Default Ring Time: 20 Sec. (1~300)

Enable Personal AA: ☑ From external call ☐ From internal call

☑ Enable Session Timer

Minimum Session Expiration: 90 Sec. (90 ~ 1800)

Session Expires: 1800 Sec. (90 ~ 86400, must > Minimum Session Expiration)

☑ Enable RTCP Support

☐ Enable DNS SRV

Each field is described in the following table.

Table 141 Configuration > PBX > Global > SIP Server

LABEL	DESCRIPTION
SIP Server Realm Name	A realm is a set of usernames and passwords used by SIP client devices to authenticate with a SIP server. The ISG50 supports a single realm. When SIP clients register with the ISG50, they must provide the name of the realm they belong to as well as the username and password. Type the realm name which the extensions that register with the ISG50 must provide for authentication.
Port	Enter the ISG50's listening port number or keep the default value. This is the port number your SIP clients need to use to register with the ISG50. You can also enter up to two different alternate ports.
Default SIP Client Registration Expiration	The ISG50 is a SIP registrar server. A SIP registrar server maintains a database of SIP identity-to-IP address (or domain name) mapping. The ISG50 checks your username, password and realm when you register. Enter the number of seconds SIP clients are registered with the ISG50 before their registration record is deleted. Make sure that the client SIP devices are configured to re-register at an interval smaller than the time set in this field. You can enter expiration times for SIP clients that use NAT as well as those that do not.
RTP Port Range	When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. Enter the listening port number(s) for RTP traffic or keep the default values. Enter the port number at the beginning of the range in the **first** field and enter the port number at the end of the range in the **second** field.
Default Ring Time	Specify for how many seconds the ISG50 sends a ringing tone to client devices for incoming calls.

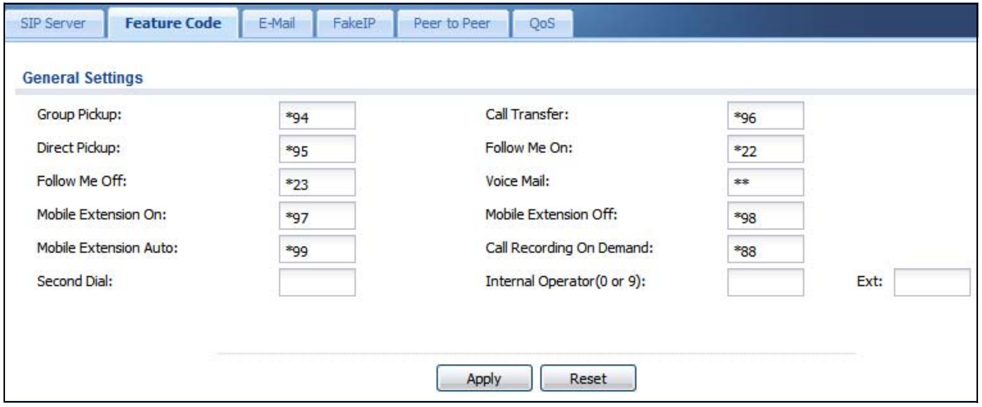
Table 141 Configuration > PBX > Global > SIP Server (continued)

LABEL	DESCRIPTION
Enable Personal AA	Select **From external call** to enable the ISG50's auto-attendant feature for calls received from outside the PBX-managed telephone system. Select **From internal call** to enable the ISG50's auto-attendant feature for calls received from within the PBX-managed telephone system.
Enable Session Timer	Select this to enable the session timer.
Minimum Session Expiration	Enter the minimum time in seconds before an idle SIP connection expires. You can enter a value between 90 and 1800.
Session Expires	Enter the duration in seconds before an idle SIP connection expires. You can enter a value between 90 and 86400. The value entered in this field must be greater than or equal to the value entered in the **Minimum SE** field.
Enable RTCP Support	Select this to have the ISG50 use RTCP (RTP Control Protocol) as an optional signalling protocol for SIP traffic.
Enable DNS SRV	Select this to have the ISG50 query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls. Doing this, however, could impact the ISG50's performance.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

27.3 The Feature Code Screen

Use this screen to set values for the feature codes the ISG50 supports from an IP phone's extension. Users can dial these codes to enable or disable the features listed below for their extension settings by entering these codes on their phone's keypad. Click **Configuration > PBX > Global > Feature Code** to open the screen as shown.

Figure 279 Configuration > PBX > Global > Feature Code



General Settings

Group Pickup: *94
Direct Pickup: *95
Follow Me Off: *23
Mobile Extension On: *97
Mobile Extension Auto: *99
Second Dial:
Call Transfer: *96
Follow Me On: *22
Voice Mail: **
Mobile Extension Off: *98
Call Recording On Demand: *88
Internal Operator(0 or 9):
Ext:

The following table describes the labels in this screen.

Table 142 Configuration > PBX > Global > Feature Code

LABEL	DESCRIPTION
Group Pickup	This code is used to pick up calls for your extension from a different extension in the same authority group.
Call Transfer	This code is used to transfer calls.
Direct Pickup	This code is used to pick up calls for your extension from a different extension.
Follow Me On	This code is used to turn the Follow Me feature on for this extension.
Follow Me Off	This code is used to turn the Follow Me feature off for this extension.
Voice Mail	This code is used to access voice mail on the ISG50.
Mobile Extension On	This code is used to activate the mobile extension feature from your regular telephone extension. Once activated, calls are sent both to your extension and to the phone designated as the mobile extension. For example, if your IP PBX extension has been configured to use your cell phone as a mobile extension, you can dial into the ISG50 with your cell phone and then enter this code. That tells the ISG50 to send all calls to your extension to your cell phone.
Mobile Extension Off	This code is used to turn off the mobile extension feature from your regular telephone extension. Calls are no longer sent simultaneously to both your extension and the mobile extension; they are sent strictly to your regular extension. For example, if all calls currently incoming to your extension are sent to your cell phone, you can dial into the ISG50 and then enter this code. That tells the ISG50 to stop sending calls intended for your extension to your cell phone.
Mobile Extension Auto	This code changes the mobile extension feature's setting from off to on or from on to off. For example, if you use this code when the mobile extension feature is turned on, it turns it off. If you use this code when the mobile extension feature is turned off, it turns it on.
Call Recording On Demand	Use this code to start recording the current call. The on-demand call recording option must also be enabled in the call recording setup. See Section 35.2 on page 545.
Second Dial	This code is used to get a second dial tone. When you enter the **Second Dial** code from your phone, the ISG50 opens a connection to the outside telephone network. For example, in many office environments you cannot access an outside dial tone unless you press "9" or "0" first. A number dialed without such a prefix is considered internal and thus routed to the appropriate extension. If that extension does not exist, an error is returned. Leave this field blank if you do not require people using your telephone network to dial a specific number to access an outside line. Note: You only need to enable this function if your phone network is analog-based (such as one that uses FXS). Digital phone systems such as SIP and BRI do not require it. Note: If you enable this function on a digital network, a person does not need to use the **Second Dial** number in conjunction with any phone numbers dialed.
Internal Operator (0 or 9)	Use the first field of this code to set which number (0 or 9) internal users dial to reach the internal operator. Use the second field to specify the operator's extension number. The extension must already exist in the ISG50.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

27.4 The E-Mail Screen

Use this screen to configure the mail server information through which the ISG50 sends voice mails and CDR (Call Detail Record) files to the email addresses which you configured in extension voice mail (see Section 29.3.3 on page 467) and CDR (see Section 54.2 on page 721) screens. Click **Configuration** > **PBX** > **Global** > **E-Mail** to view the screen as shown next.

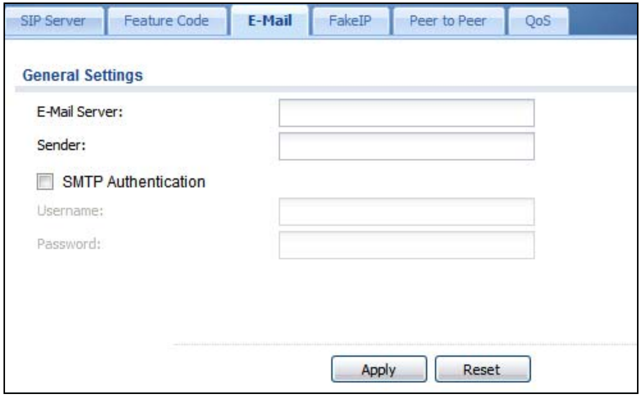

SIP Server
Feature Code
E-Mail
FakeIP
Peer to Peer
QoS
General Settings
E-Mail Server:
Sender:
☐ SMTP Authentication
Username:
Password:
Apply
Reset

Figure 280 Configuration > PBX > Global > E-Mail

Each field is described in the following table.

Table 143 Configuration > PBX > Global > E-Mail

LABEL	DESCRIPTION
E-Mail Server	Specify a mail server’s IP address.
Sender	Specify the sender’s email address.
SMTP Authentication	Select this and enter your username and password if user authentication is required in the mail server.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

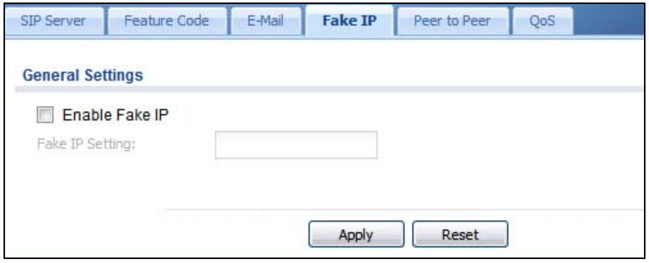
27.5 The Fake IP Screen

Use this screen to configure settings that may help you to avoid any potential VoIP problems that result from having your ISG50 behind a NAT router.

Note: This feature should be used if the NAT router does not utilize SIP ALG.

Click **Configuration** > **PBX** > **Global** > **Fake IP** to view the screen as shown next.

Figure 281 Configuration > PBX > Global > Fake IP


SIP Server
Feature Code
E-Mail
Fake IP
Peer to Peer
QoS
General Settings
☐ Enable Fake IP
Fake IP Setting:
Apply
Reset

Each field is described in the following table.

Table 144 Server > Fake IP

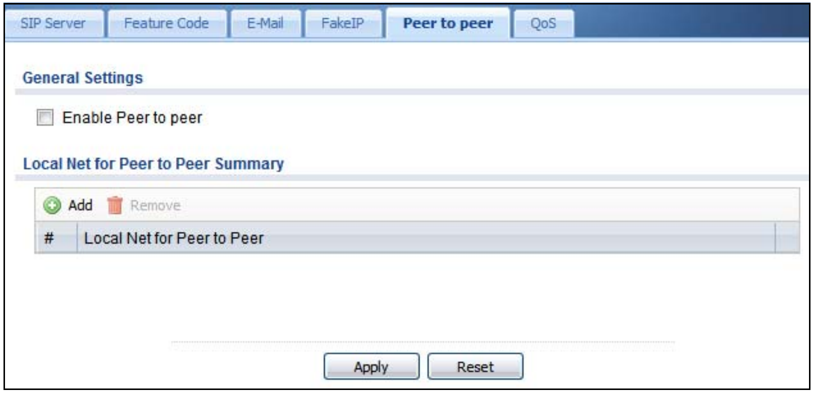
LABEL	DESCRIPTION
Enable Fake IP	Turn on fake IP to have the ISG50 replace the IP address inside all outgoing SIP packets with the IP address of the upstream NAT router on your network. When the packets get to their destination, the destination device can send its response to the embedded address of the NAT router. The NAT router then forwards the packets downstream to the ISG50, which in turn sends them to the device on the local end of the telephone conversation. If you enable it, you must assign a value to the **Fake IP Setting** field.
Fake IP Setting	Enter the public IP address that the upstream NAT router uses to send out the ISG50's SIP traffic. This is the IP address that will be inserted into all outgoing SIP traffic.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

27.6 The Peer to Peer Screen

Use this screen to allow the ISG50 to set up a direct connection between two IP phones on the same subnet. This allows the ISG50 to remain free of the loading burden and free up IP PBX resources (such as DSP channels). When a special feature request is made by either end of the connection, such as call parking or music on hold, then the ISG50 re-establishes control of the connection to implement the feature.

Click **Configuration > PBX > Global > Peer to Peer** to view the screen as shown next.

Figure 282 Configuration > PBX > Global > Peer to Peer


SIP Server
Feature Code
E-Mail
FakeIP
Peer to peer
QoS
General Settings
☐ Enable Peer to peer
Local Net for Peer to Peer Summary
Add
Remove
#
Local Net for Peer to Peer
Apply
Reset

Each field is described in the following table.

Table 145 Configuration > PBX > Global > Peer to Peer

LABEL	DESCRIPTION
Enable Peer to Peer	Select this to have the ISG50 to set up direct connections between two IP phones on the same subnet. If you enable it, you should set up the **Local Net for Peer to Peer**.
Local Net for Peer to peer	
Add	Click this to add a new entry to the local net list.
Remove	Click this to delete the selected item(s) in this list.
#	This field is a sequential value and is not associated with a specific entry.
Local Net for Peer to Peer	This displays the network on which Peer to Peer connections may be made. For example, if the Local Net IP address is 192.168.1.0/24, then any device with an IP from 192.168.1.1 to 192.168.1.254 can make a peer connection to any other device in the same host range.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

27.6.1 How the Peer-to-Peer SIP Connection Works

The following is a basic explanation of how the ISG50 creates a peer-to-peer SIP connection between two IP phones within the same host range.

1 The first phone (**A**) sends an invite for the other phone to the ISG50. This invite includes its IP address and which codecs it can use.

2 Next, the ISG50 accepts the invite on behalf of the second phone (**B**) and sends an acknowledgement back to **A**.

3 The ISG50 sends an new invite to **B**. This invite includes the ISG50's IP address and the codecs it has in common in with **A**.

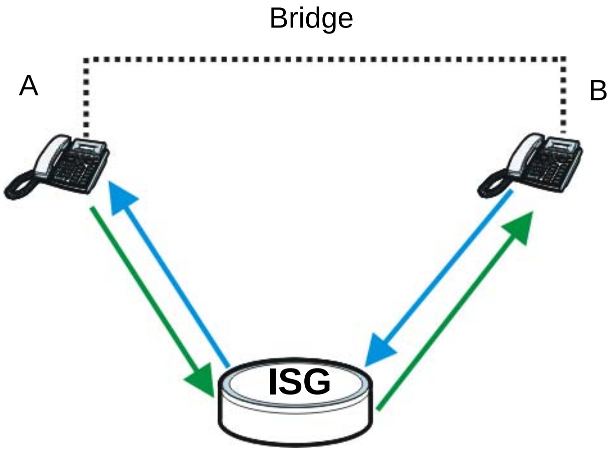
For example, if **A** says it can use the G.723, Speex, and GSM codecs but the ISG50 is set to G.723, then the ISG50 lets **B** know that only the G.723 codec is available for the telephone call.

4 When **B** accepts the invite from the ISG50, it sends back an acknowledgement. The ISG50 has now received confirmation from both phones of their IP addresses and an mutually agreed upon codec.

5 The ISG50 sends out a re-invite to both **A** and **B** that includes both IP addresses and the codec to be used. This allows the two phones to create a bridge directly with one another. The ISG50 then removes itself from the communication chain.

Note: If either phone A or B requests to use a feature specific to the ISG50, such as call parking or music on hold, the ISG50 interrupts the direct communication bridge and re-establishes control of the two SIP connections.

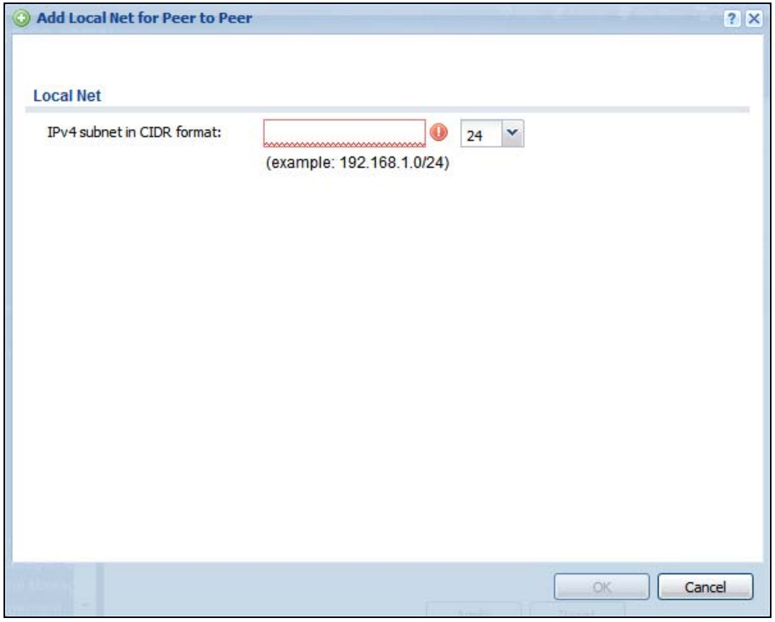
Figure 283 A Peer-to-Peer Example



27.6.2 Add Peer-to-Peer Local Net

Use this screen to add a subnet IP address to the localnet table for making peer-to-peer connections. To access this screen, click **Configuration** > **PBX** > **Global** > **Peer to Peer and click the Add icon in the Local Net for Peer to Peer** table.

Figure 284 Configuration > PBX > Global > Peer to Peer > Add



IPv4 subnet in CIDR format: 24

(example: 192.168.1.0/24)

Each field is described in the following table.

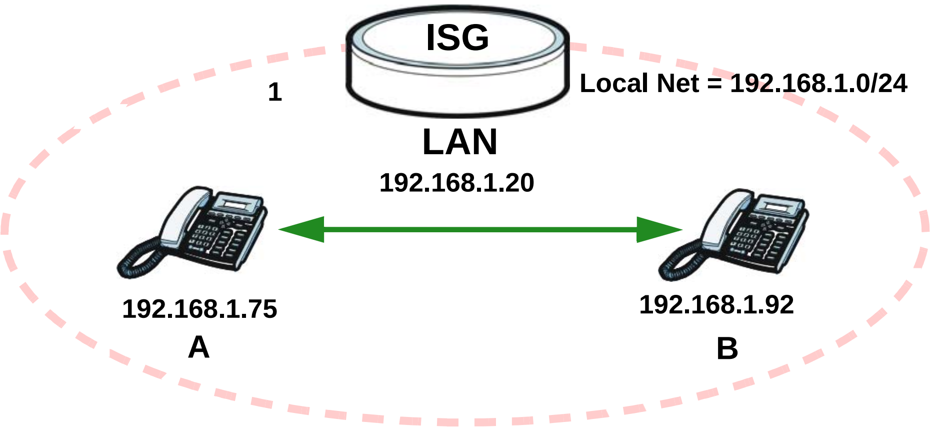
Table 146 Configuration > PBX > Global > Peer to Peer > Add

LABEL	DESCRIPTION
IPv4 subnet in CIDR format	Enter an IPv4-compatible IP address in this field then select the length of the subnet mask from the list. This option defines a subnet for which the ISG50 can set up peer-to-peer networking.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

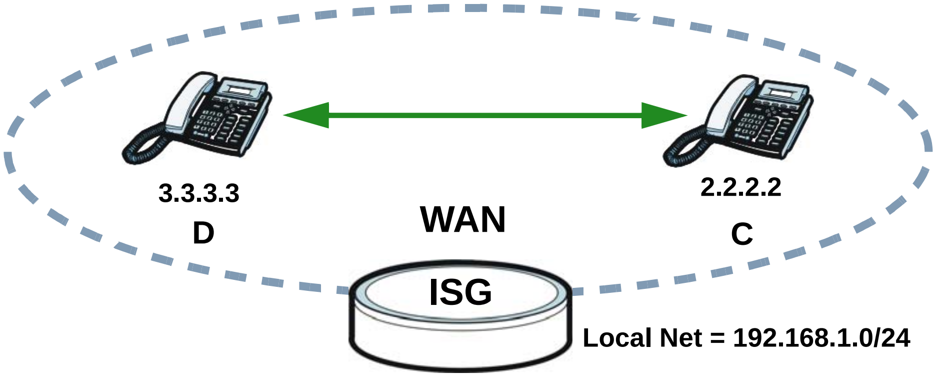
27.6.3 How Local Net and Peer-to-Peer Work Together

Peer-to-peer calls can be made through the ISG50, but with certain limitations:

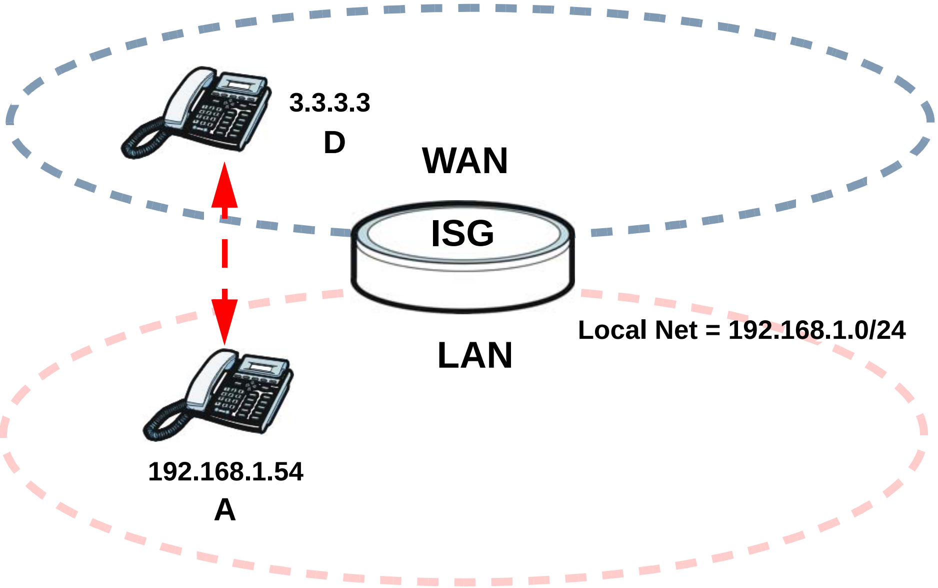
1 Peer-to-peer calls can be made between any devices on the LAN if they belong to a subnet listed in the same localnet table.


ISG
1
Local Net = 192.168.1.0/24
LAN
192.168.1.20
192.168.1.75
A
192.168.1.92
B

2 Peer-to-peer calls can be made between devices on the WAN if neither device belongs to a subnet listed in the localnet table.


3.3.3.3
D
2.2.2.2
C
WAN
ISG
Local Net = 192.168.1.0/24

3 However, peer-to-peer calls cannot be made between devices if one of them belongs to a subnet listed in the localnet table and the other does not.


3.3.3.3
D
WAN
ISG
Local Net = 192.168.1.0/24
LAN
192.168.1.54
A

Furthermore, the devices making a peer-to-peer connection:

- Must have a common codec they can use between them.
- Must use SIPInfo for DTMF.
- Must not be using NAT.

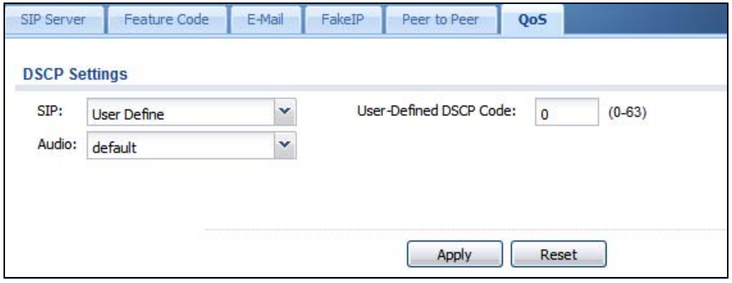
If they cannot meet these conditions, the peer-to-peer connection will fail and the call will be routed through the ISG50 instead.

For more information on adding different subnets to the localnet table, see Section 27.6 on page 436.

27.7 The QoS Screen

Use this screen to set up DSCP settings for SIP and audio traffic. To access this screen, click **Configuration > PBX > Global > QoS**.

Figure 285 Configuration > PBX > Global > QoS


SIP Server
Feature Code
E-Mail
FakeIP
Peer to Peer
QoS
DSCP Settings

SIP: User Define

User-Defined DSCP Code: 0 (0-63)

Audio: default

Apply
Reset

Each field is described in the following table.

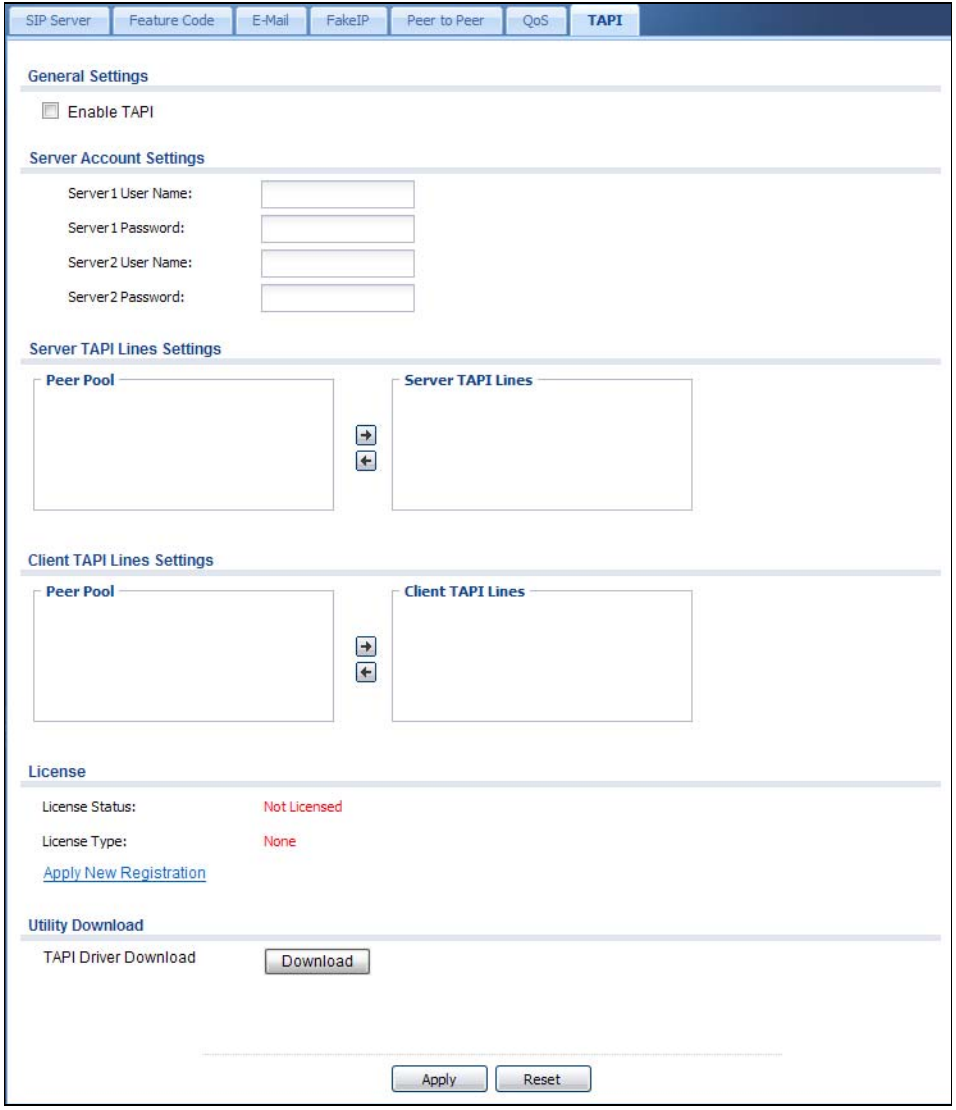
Table 147 Configuration > PBX > Global > QoS

LABEL	DESCRIPTION
SIP	Select the DSCP value to mark outgoing SIP control packets. You can choose one of the **AF** (Assured Forwarding) values or select **User Define** to specify another DSCP value. When the ISG50 auto provisions phones it sets them to mark outgoing SIP control packets with this DSCP value.
Audio	Select the DSCP value to mark outgoing SIP audio payload packets. You can choose one of the **AF** (Assured Forwarding) values or select **User Define** to specify another DSCP value. When the ISG50 auto provisions phones it sets them to mark outgoing SIP audio payload packets with this DSCP value.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

27.8 The TAPI Screen

Use this screen to enable TAPI, configure TAPI line settings on the ISG50 and download the ZyXEL TAPI driver. To access this screen, click **Configuration > PBX > Global > TAPI**.

Figure 286 Configuration > PBX > Global > TAPI



SIP Server
Feature Code
E-Mail
FakeIP
Peer to Peer
QoS
TAPI
General Settings
☐ Enable TAPI
Server Account Settings
Server1 User Name:
Server1 Password:
Server2 User Name:
Server2 Password:
Server TAPI Lines Settings
Peer Pool
Server TAPI Lines
Client TAPI Lines Settings
Peer Pool
Client TAPI Lines
License
License Status:
Not Licensed
License Type:
None
Apply New Registration
Utility Download
TAPI Driver Download
Download
Apply
Reset

Each field is described in the following table.

Table 148 Configuration > PBX > Global > TAPI

LABEL	DESCRIPTION
Enable TAPI	Select this option to activate TAPI on the ISG50. You should register the ISG50 and activate the TAPI service first in the **Configuration > Licensing > Registration** screen.
Server1/2 User Name	Specify the user name for the TAPI server account. Users log in with the server account using the TAPI utility can act as a TAPI server and manage multiple TAPI lines at a time. You can use alphanumeric and -_@. characters, and it can be up to 30 characters long.

Table 148 Configuration > PBX > Global > TAPI (continued)

LABEL	DESCRIPTION
Server1/2 Password	Specify the password for the TAPI server account. You can use up to 63 printable ASCII characters.
Server TAPI Lines Settings	**Peer Pool** lists all the extension numbers that you created in the **Authority Group > Add** screen (see Section 29.3.1 on page 462). Select the extensions that you want a TAPI server to manage via a TAPI connection, and click the right arrow button to add them. **Server TAPI Lines** lists the extensions a TAPI server can manage. Select any extensions that you don't want the TAPI server to manage and monitor, and click the left arrow button to exclude them.
Client TAPI Lines Settings	**Peer Pool** lists all the extension numbers that you created in the **Authority Group > Add** screen. Select the extensions that you want a TAPI client to manage via a TAPI connection, and click the right arrow button to add them. **Client TAPI Lines** lists the extensions that can be managed by TAPI clients. Select any extensions that you don't want the TAPI client to manage and monitor, and click the left arrow button to exclude them.
License Status	This field displays whether the TAPI service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**).
License Type	This field displays whether you applied for a trial application (**Trial**) or registered the service with your iCard's PIN number (**Standard**). This field shows **None** when the service is not activated.
Apply New Registration	Click this button to open the **Registration** screen where you can register the device and activate or extend a service.
TAPI Driver Download	Click the **Download** button to get the ZyXEL TAPI driver from the ZyXEL FTP site. Make sure your ISG50 has Internet access. Note: Before or after you install the TAPI driver and utility in your computer, you need to activate the TAPI service and create a server account or extension on the ISG50 in order to communicate with the ISG50 using TAPI connections.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

27.8.1 Setting Up the TAPI Driver and Utility on Your Computer

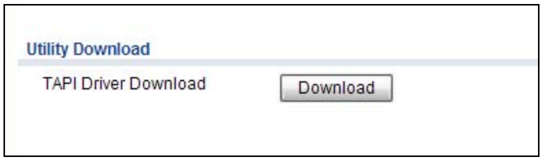
Your computer needs to be running Windows XP, Windows Vista, Windows 7 or Windows Server 200x.

Note: If your computer is on the ISG50's WAN and you want to have a TAPI connection to the ISG50, make sure a firewall rule for the CTI port service object is configured to allow incoming TCP port 5038 traffic.

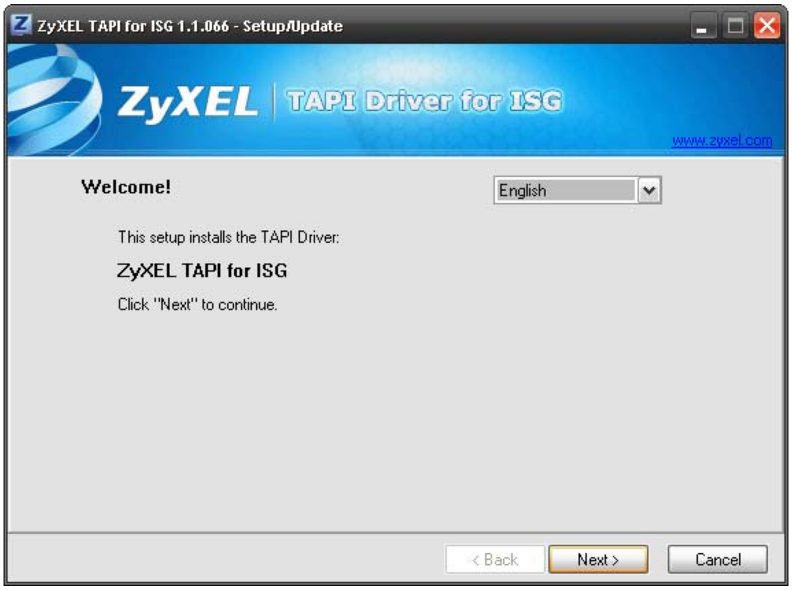
Note: If you need to install the TAPI driver on a computer that is running a 64-bit operating system, and see a message "This application has failed to start because its side-by-side configuration is incorrect.", download and install the "Microsoft Visual C++ 2005 SP1 Redistributable Package (x64)" from the Microsoft website.

To download and install the driver:

1 Click **Configuration > PBX > Global > TAPI**. Click **Download** and save the file to your computer.


Utility Download
TAPI Driver Download
Download

2 Unzip the file and run it, following the on-screen instructions to install it.


ZyXEL TAPI for ISG 1.1.066 - Setup/Update
ZyXEL
TAPI Driver for ISG
www.zyxel.com
English
< Back
Next >
Cancel

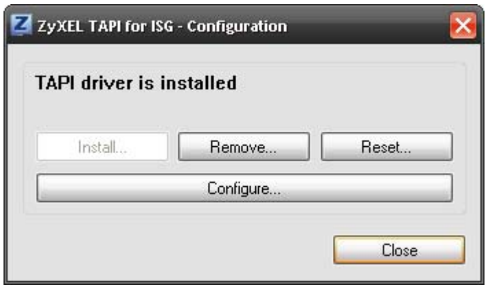
Welcome!

This setup installs the TAPI Driver:

ZyXEL TAPI for ISG

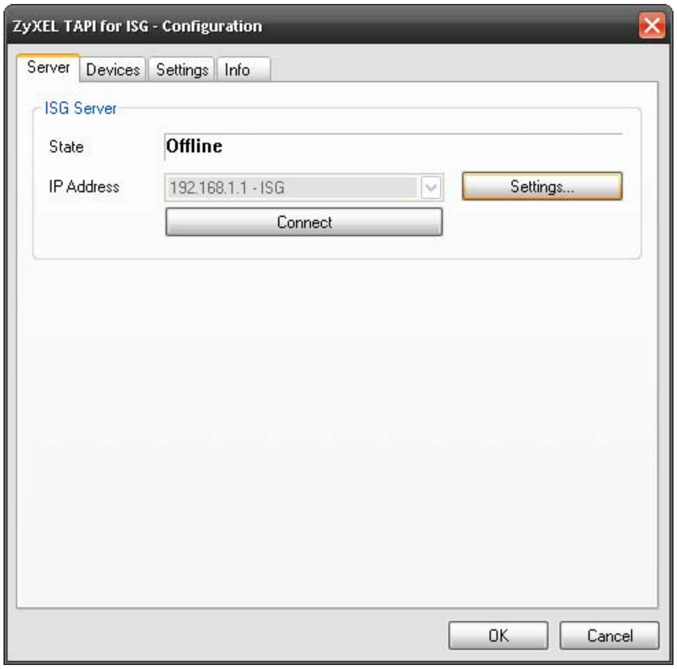
Click "Next" to continue.

3 Open the ZyXEL_TAPI_for_ISG utility and click **Configure...**.


ZyXEL TAPI for ISG - Configuration
Install...
Remove...
Reset...
Configure...
Close

TAPI driver is installed

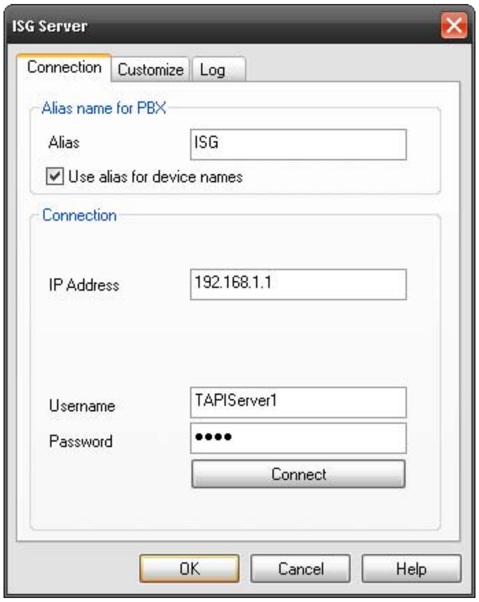
4 In the **Server** window, click **Settings...**.


ZyXEL TAPI for ISG - Configuration
Server
Devices
Settings
Info
ISG Server
Settings...
Connect
OK
Cancel

State Offline

IP Address 192.168.1.1 - ISG

5 Enter the ISG50's host name and IP address. If you want the computer to work as a TAPI server and manage more than one extension, enter the user name and password for a server account already configured in the ISG50. If you want the computer to work as a TAPI client, enter the number of an existing extension and its password. Click **Connect** and **OK**.


ISG Server
Connection
Customize
Log
Alias name for PBX
Connection
Connect
OK
Cancel
Help

Alias ISG

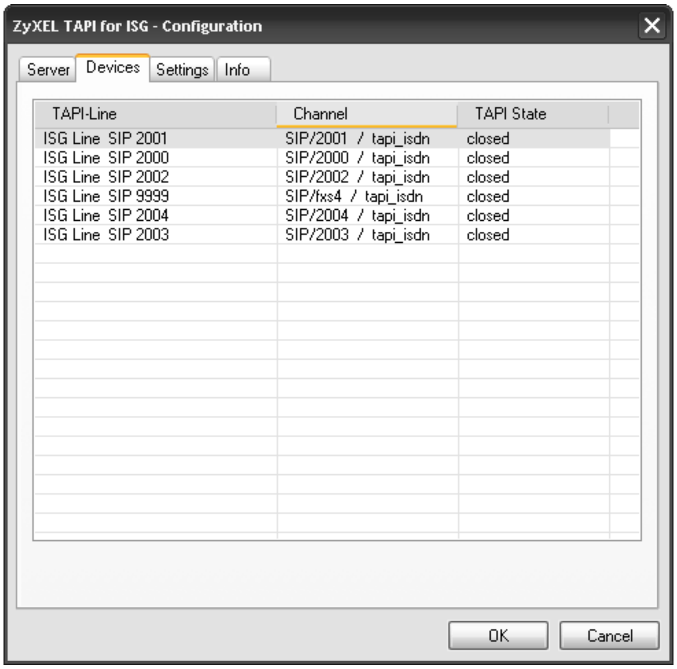
☑ Use alias for device names

IP Address 192.168.1.1

Username TAPIServer1

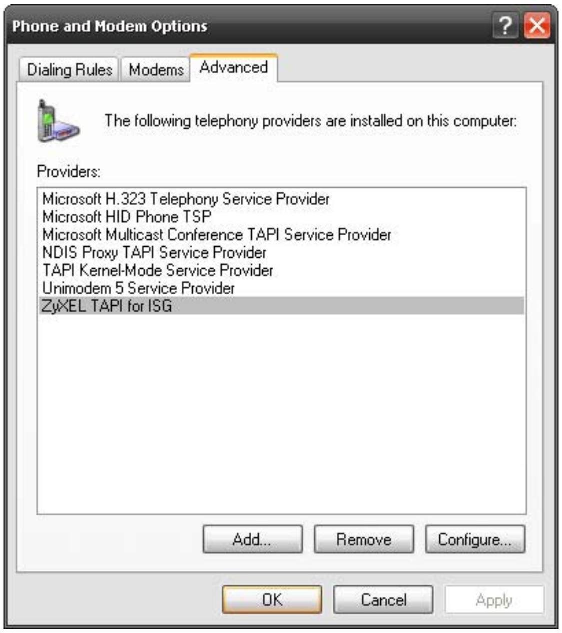
Password ••••

6 In the **Devices** window, you can view the state and channel for the TAPI lines that you can control and manage. To change the TAPI line state or make/answer a call, you need the CTI (Computer Telephony Integration) client or server software, such as xtelsio CTI Client or ESTOS UCServer.


ZyXEL TAPI for ISG - Configuration
Server
Devices
Settings
Info
OK
Cancel

TAPI-Line	Channel	TAPI State
ISG Line SIP 2001	SIP/2001 / tapi_isdn	closed
ISG Line SIP 2000	SIP/2000 / tapi_isdn	closed
ISG Line SIP 2002	SIP/2002 / tapi_isdn	closed
ISG Line SIP 9999	SIP/fxs4 / tapi_isdn	closed
ISG Line SIP 2004	SIP/2004 / tapi_isdn	closed
ISG Line SIP 2003	SIP/2003 / tapi_isdn	closed

To confirm that the TAPI driver is installed, click **start > Control Panel > Phone and Modem Options**. Then click the **Advanced** tab and make sure a ZyXEL TAPI entry appears in the list of providers.


Phone and Modem Options
Dialing Rules
Modems
Advanced
Add...
Remove
Configure...
OK
Cancel
Apply

The following telephony providers are installed on this computer:

Providers:

Microsoft H.323 Telephony Service Provider
Microsoft HID Phone TSP
Microsoft Multicast Conference TAPI Service Provider
NDIS Proxy TAPI Service Provider
TAPI Kernel-Mode Service Provider
Unimodem 5 Service Provider
ZyXEL TAPI for ISG

27.9 Network Technical Reference

This section contains background material relevant to the **Server** screens.

ISDN Overview

ISDN (Integrated Service Digital Network) is a circuit-switched telephone network system. In ISDN, there are two types of channels: B-channels and D-channels. ISDN allows digital transmission of voice, video and data over ordinary telephone copper wires using B-channels with 64 kbps bandwidth. D-channels are mainly used for signaling and control with 16 kbps or 64 kbps bandwidth depending on service levels.

The ISG50 supports the BRI ISDN service level. BRI (Basic Rate Interface) contains two 64 kbps B channel and one 16 kbps D channel (2B+1D). A BRI user can have up to 128 kbps service.

DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets (based on the application types and traffic flow) so that they receive specific per-hop treatment at DiffServ-compliant network devices along their route. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different forwarding treatment. Resources can then be allocated according to the DSCP values and the configured policies.

The ISG50 allows you to mark outgoing frames with following PHB classifications:

Assured Forwarding (AF) - This is a PHB group allowing you to choose from one of four classes of forwarding assurance. Each class has three choices of drop precedence to choose from. When congestion occurs, the DS nodes on your network treat all IP packets marked with the same class and drop precedence identically. DS nodes can be configured to protect packets with lower drop precedence value by discarding packets with a higher drop precedence value.

Expedited Forwarding (EF) - The EF PHB defines a single DSCP designed for simulating a private end-to-end pipeline across a DiffServ network. IP packets are marked for high priority low-loss, low-latency, low-jitter, assured-bandwidth end to end service through DS domains. This is recommended for use with VoIP traffic as it addresses the factors that cause degradation in sound quality.

Class Selector (CS) - IP packets are marked with values partially backwards-compatible with known current uses of IP precedence field. The packets marked with higher values are given higher priority than those with lower values.

28

Voice Interfaces

28.1 Overview

This chapter shows you how to configure parameters for FXO/FXS, and ISDN BRI channels.

28.1.1 What You Can Do in this Chapter

- Use the **FXS** screen to configure the ISG50's FXS ports for connecting analog phones to your ISG50. See Section 28.2 on page 449.
- Use the **FXO** screen to configure the ISG50's FXO ports for connecting to a traditional PBX's FXS ports. See Section 28.3 on page 450.
- Use the **BRI** screen to configure the BRI line settings to the peer device your ISG50 connects to. See Section 28.4 on page 451.

28.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

FXO Channel

An FXO channel is a connection from the ISG50 to a traditional PBX (for example a PSTN connection) via one of the FXO ports installed on the ISG50. You must configure how the ISG50 adjusts the signal volume sent to and received from a traditional PBX.

FXS Channel

An FXS channel is a connection from on of the ISG50's FXS ports to an analog phone. You can configure how the ISG50 adjusts the signal volume sent to and received from a connected device such as an analog phone or a PBX.

BRI

BRI (Basic Rate Interface) is an Integrated Services Digital Network (ISDN) physical layer standard and used to transmit voice and user data. BRI is used in homes or small companies providing data rates up to 128 kbps.

TE/NT

TE (Terminal Equipment) refers to an ISDN user device such as an ISDN telephone, video telephone, digital fax machine (also known as G4 fax machine). The NT (Network Terminal) is the termination device between TEs and the ISDN central office (CO). The NT is responsible for performance, monitoring, power transfer, and multiplexing of the channels. You must connect a TE device to a NT device to access an ISDN network. The ISG50 is a TE device.

Types of ISDN Switches

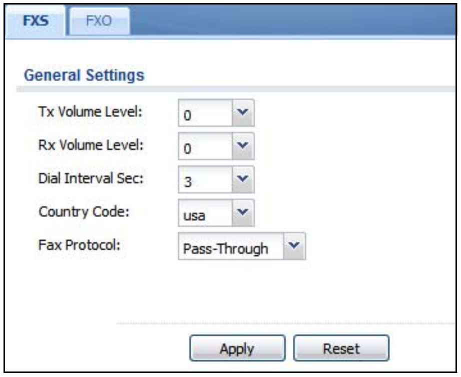
There are many different ISDN switch types from different vendors in the world. The BRI interface enables the ISG50 to communicate with the following BRI switches.

- 5ESS - AT&T basic rate switches
- MDS100
- NI1 - National ISDN-1 switches
- ENT3 - Euro-ISDN switches (UK and others)
- AUS - Australian TS013 switches

28.2 The FXS Screen

Use this screen to configure settings for the analog phones connected to the ISG50. To access this screen, click **Configuration > PBX > Voice Interfaces > FXS**.

Figure 287 Configuration > PBX > Voice Interfaces > FXS



Tx Volume Level: 0
Rx Volume Level: 0
Dial Interval Sec: 3
Country Code: usa
Fax Protocol: Pass-Through

Each field is described in the following table.

Table 149 Configuration > PBX > Voice Interfaces > FXS

LABEL	DESCRIPTION
Tx Volume Level	Select the volume level transmitted from the ISG50. -6 is the quietest, and 6 is the loudest.
Rx Volume Level	Select the volume level transmitted to the ISG50. -6 is the quietest, and 6 is the loudest.
Dial Interval Sec	Enter the number of seconds the ISG50 should wait after you stop dialing numbers (from FXS extensions) before it makes the phone call.
Country Code	The signals used by telephone companies to indicate a busy line or an available line differ by country. You must select the country code for the location of the ISG50. The ISG50 can then detect whether the FXS line is in use or available. Select **default** to reset the country code value to the factory defaults.
Fax Protocol	Select **Pass-Through** to use UDP packets with G.711 format or T.38 format to send fax messages. T.38 provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.

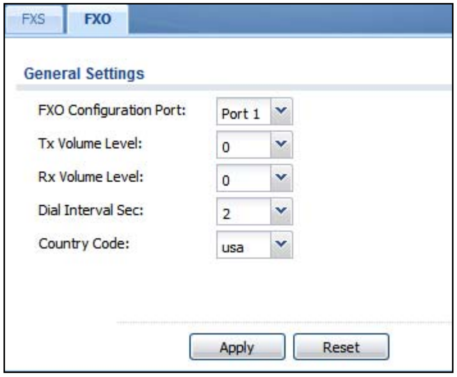
Table 149 Configuration > PBX > Voice Interfaces > FXS (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

28.3 The FXO Screen

Use this screen to configure settings related to the FXO lines configured on the ISG50. To access this screen, click **Configuration** > **PBX > Voice Interfaces > FXO**.

Figure 288 Configuration > PBX > Voice Interfaces > FXO



FXO Configuration Port: Port 1
Tx Volume Level: 0
Rx Volume Level: 0
Dial Interval Sec: 2
Country Code: usa

Each field is described in the following table.

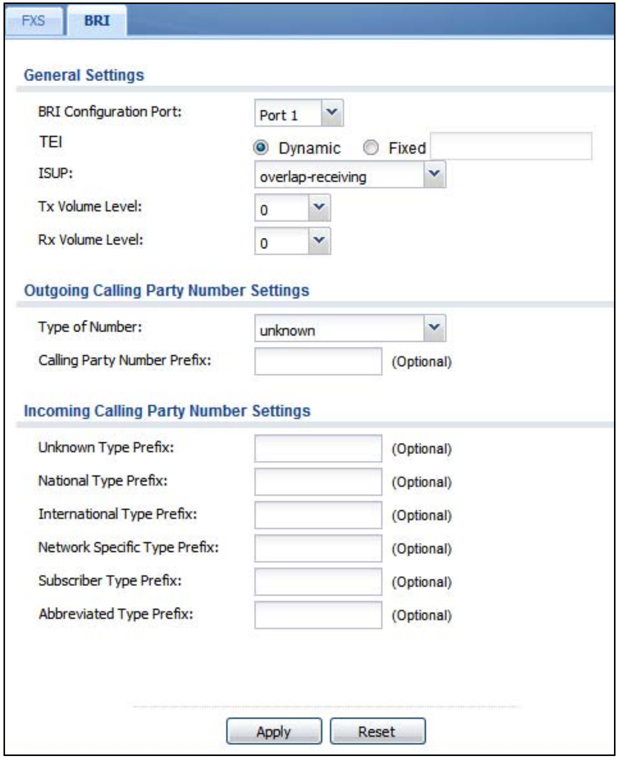
Table 150 Configuration > PBX > Voice Interfaces > FXO

LABEL	DESCRIPTION
FXO Configuration Port	Specify the FXO port to configure.
TX Volume	Select the volume level transmitted from the ISG50. -6 is the quietest, and 6 is the loudest.
RX Volume	Select the volume level transmitted to the ISG50. -6 is the quietest, and 6 is the loudest.
Dial Interval Sec	Enter the number of seconds the ISG50 should wait after you stop dialing numbers (from FXO extensions) before it makes the phone call.
Country Code	The signals used to indicate a busy line or an available line differ by country. You must select the country code for the location of the ISG50. The ISG50 can then recognize whether the FXO line is in use or available. Select **default** to reset the country code value to the factory defaults.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

28.4 The BRI Screen

Use this screen to configure ISDN BRI interface settings on the ISG50. Click **Configuration** > **PBX** > **Voice Interfaces** > **BRI** to view the screen as shown next.

Figure 289 Configuration > PBX > Voice Interfaces > BRI



General Settings

BRI Configuration Port: Port 1

TEI ● Dynamic ○ Fixed

ISUP: overlap-receiving

Tx Volume Level: 0

Rx Volume Level: 0

Outgoing Calling Party Number Settings

Type of Number: unknown

Calling Party Number Prefix: (Optional)

Incoming Calling Party Number Settings

Unknown Type Prefix: (Optional)

National Type Prefix: (Optional)

International Type Prefix: (Optional)

Network Specific Type Prefix: (Optional)

Subscriber Type Prefix: (Optional)

Abbreviated Type Prefix: (Optional)

Each field is described in the following table.

Table 151 Configuration > PBX > Voice Interfaces > BRI

LABEL	DESCRIPTION
BRI Configuration port	Specify the BRI port to configure.
TEI	This Terminal Endpoint Identifier is used to uniquely identify each TE device. Select **Dynamic** to automatically request an ID when the ISG50 is connected to the network. Or select **Fixed** and enter a number (0-63) provided from your telephone company. Note: You must configure the same TEI on the ISG50 and its connected BRI device.
ISUP	Specify the signalling method the ISG50 accepts to receive a callee's number through a specified BRI port. **en-bloc**: The ISG50 expects to receive a complete callee's number at one time. **overlap-receiving**: The ISG50 expects to receive digits of a callee's number one-by-one.
Tx Volume Level	Select the volume level transmitted from the ISG50. -6 is the lowest, and 6 is the loudest.
Rx Volume Level	Select the volume level transmitted to the ISG50. -6 is the lowest, and 6 is the loudest.
Outgoing Calling Party Number Settings	Use this section to configure your outgoing calling party numbers.

Table 151 Configuration > PBX > Voice Interfaces > BRI (continued)

LABEL	DESCRIPTION
Type of Number	Select the type for the prefix number which might be required by your telephone company to make outgoing calls. The options you can select are **abbreviated**, **unknown**, **international**, **national**, **network-specific**, and **subscriber**.
Calling Party Number Prefix	Enter a number to add in the beginning of the outgoing caller's numbers using this trunk line. This field can be 0-20 digits in length.
Incoming Calling Party Number Settings	Use this section to set your incoming calling party number prefixes.
Unknown Type Prefix	Specify the prefix to add to the calling party numbers of incoming calls of unknown type.
National Type Prefix	Specify the prefix to add to the calling party numbers of incoming national calls.
International Type Prefix	Specify the prefix to add to the calling party numbers of incoming international calls.
Network Specific Type Prefix	Specify the prefix to add to the calling party numbers of incoming network-specific calls.
Subscriber Type Prefix	Specify the prefix to add to the calling party numbers of incoming subscriber calls.
Abbreviated Type Prefix	Specify the prefix to add to the calling party numbers of incoming abbreviated calls.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

29

Extension Management

29.1 Overview

This chapter shows you how to configure settings for managing groups of extensions.

29.1.1 What You Can Do in this Chapter

- Use the **Authority Group** screen to set up, configure and manage the ISG50's authority groups. See Section 29.2 on page 458.
- Use the **Group Access Code** screen to configure the codes that unlock access to each authority group's privileges. See Section 29.4 on page 471.
- Use the **Click-To-Talk** screen to set up CTT groups and their associated extensions.

29.1.2 What You Need to Know

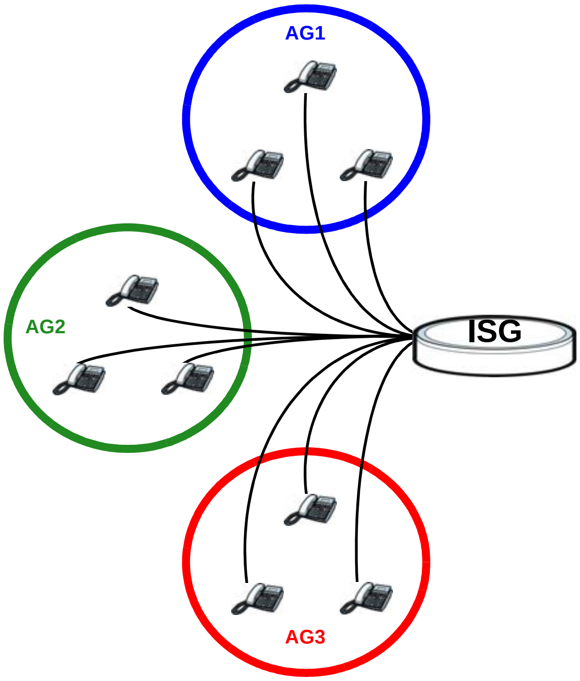
The following terms and concepts may help you as you read through the chapter.

Authority Groups

You must create at least one authority group on the ISG50 before you can create extensions. See Section 6.1.1.1 on page 87 for an overall explanation of authority groups and extensions. This chapter focuses on how to create authority groups on the ISG50.

The following figure shows the ISG50’s extensions divided into three authority groups (**AG1**, **2** and **3**). Each authority group can have different settings and privileges.

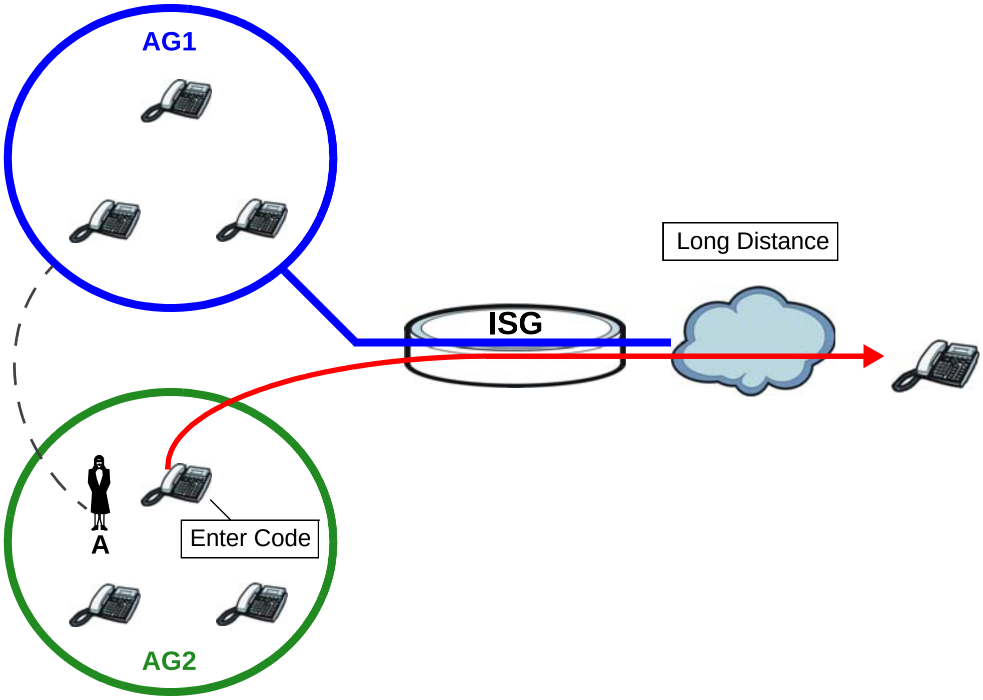
Figure 290 Authority Group Overview



The group access code allows you to use the outbound dialing rules assigned to your authority group from extensions that do not have the same outbound dialing rules assigned to them.

The following figure shows user **A**, who is a member of authority group **AG1** (which has the ability to make long distance calls) moving to a phone belonging to authority group **AG2** (which cannot make long distance calls). She enters the code number and is able to place a call over the long distance connection.

Figure 291 Call Access Code Overview



Group Access Codes

Group access codes allow your authority group members to use their group's privileges with whichever extension they are using.

For example, you belong to an authority group allowed to make both local and long distance calls from your extension. Your secretary, however, belongs to a different authority group and can make only local calls. When you try to make a long distance call from your secretary's extension the ISG50 does not allow it and prompts you to enter the access code associated with your authority group. After you enter the access code, the ISG50 completes your long distance call without you having to re-dial it.

Authority Groups and Extensions

Basically, you can think of an authority group as a set of extensions. You use an authority group to assign equal rights to the entire set of extensions. Thus, an authority group is a group of extensions that all have the same authority. For example, if you create two authority groups, you can allow one group to make local calls and long distance calls and the second authority group to make local calls only.

Authority Group Guidelines

Authority groups and extensions follow these guidelines:

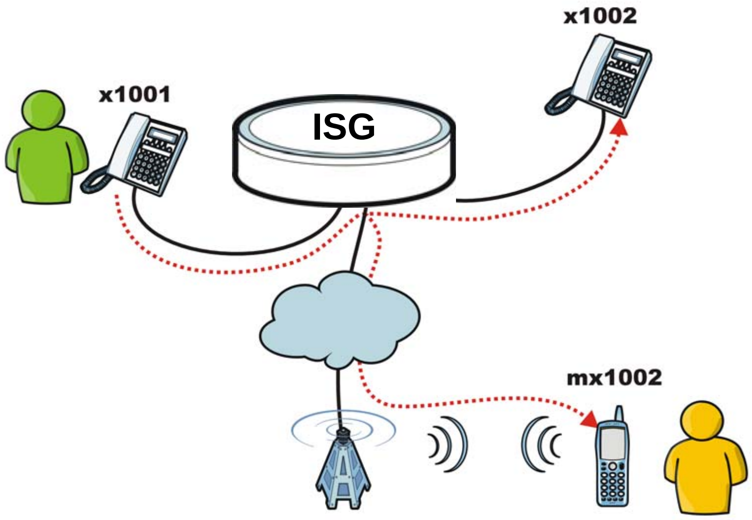
- You must create at least one authority group on the ISG50.

- Each extension can be a member of only one authority group.
- SIP and FXS extensions are treated the same within an authority group.

Mobile Extensions

A mobile extension is essentially call forwarding to both your IP phone extension and another phone. When you set up a mobile extension and then activate it from your IP phone using a feature code (Section 27.3 on page 433), all calls sent to your IP phone extension are also sent at the same time to the phone that is designated as your mobile extension. When the call is picked up on one phone, the ISG50 stops ringing the other.

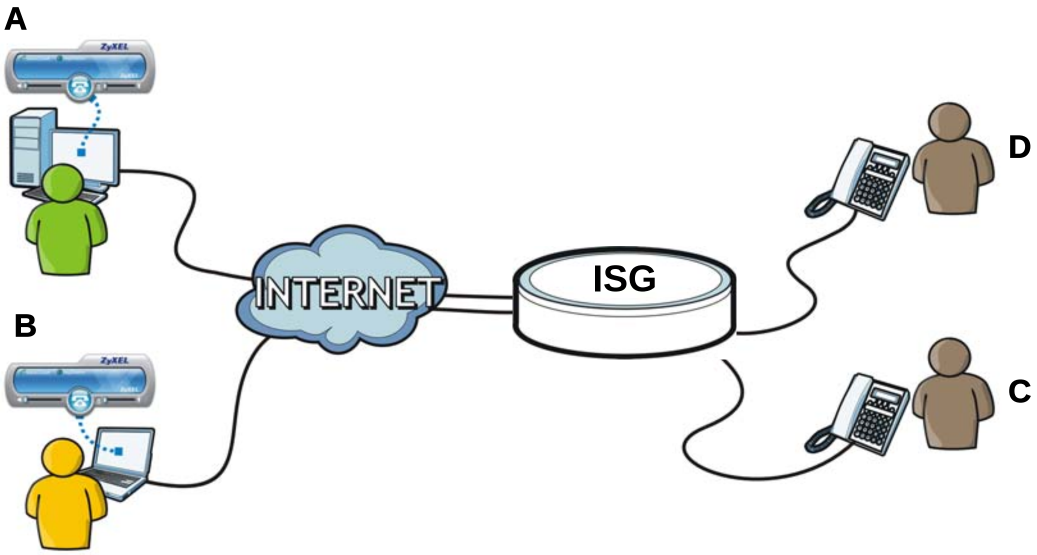
Figure 292 A Mobile Extension Example



Click-To-Talk (CTT)

A Click-To-Talk (CTT) group allows visitors to your website to click an HTML link to use a web-based IP phone to connect to the CTT group's extensions.

Figure 293 A Click-To-Talk Example



For example, users **A** and **B** click on an embedded Click-To-Talk link on a company's online ordering web page, the web-based IP phone opens and lets them talk to the the CTT group's extensions (sales agents **C** and **D** in this example). A caller must use a microphone with his computer.

Finding Out More

- See Section 29.3 on page 461 for more information on features related to individual extensions.
- See Section 29.6 on page 475 for technical reference information on voice and video codecs.

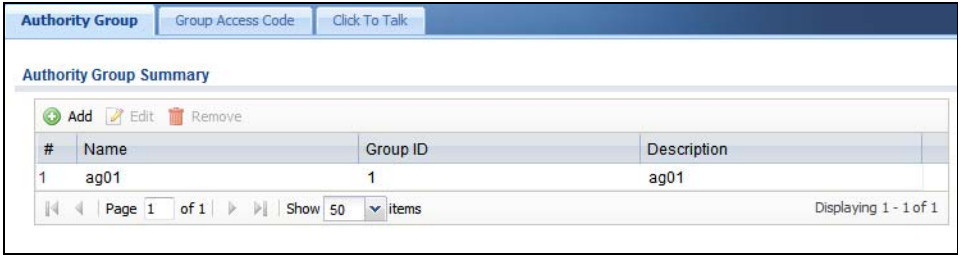
29.1.3 Before You Begin

To use the Click-To-Talk feature, you must have a valid license key for the number of CTT accounts that you wish to enable. You can get a license by purchasing a Click-To-Talk iCard from your local ZyXEL product vendor. Be sure that you have purchased a license for the number of CTT extensions you want to use, and that your registration information on the licensing page is up to date (see Chapter 11 on page 229)

29.2 The Authority Group Screen

Use this screen to set up authority groups on the ISG50. To access this screen, click **Configuration > PBX > Extension Management > Authority Group**.

Figure 294 Configuration > PBX > Extension Management > Authority Group


Authority Group
Group Access Code
Click To Talk
Authority Group Summary
Add
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1

#	Name	Group ID	Description
1	ag01	1	ag01

Each field is described in the following table.

Table 152 Configuration > PBX > Extension Management > Authority Group

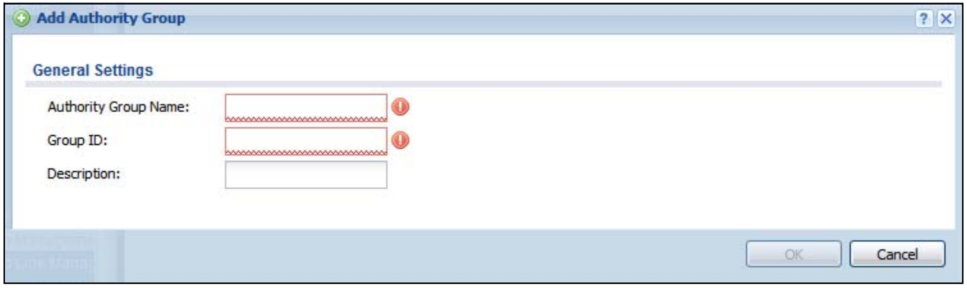
LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This is the name of the authority group.
Group ID	This is the authority group's identification number.
Description	This field displays the description for this authority group.

29.2.1 The Add Authority Group Screen

Use the **Add Authority Group** screen to create a new authority group. Click the **Add** icon in the **Authority Group** screen to view the screen as shown.

Note: Only the **Add Authority Group** screen is shown in the following figure.

Figure 295 Add Authority Group


Add Authority Group
General Settings
Authority Group Name:
Group ID:
Description:
OK
Cancel

Each field is described in the following table.

Table 153 Add Authority Group

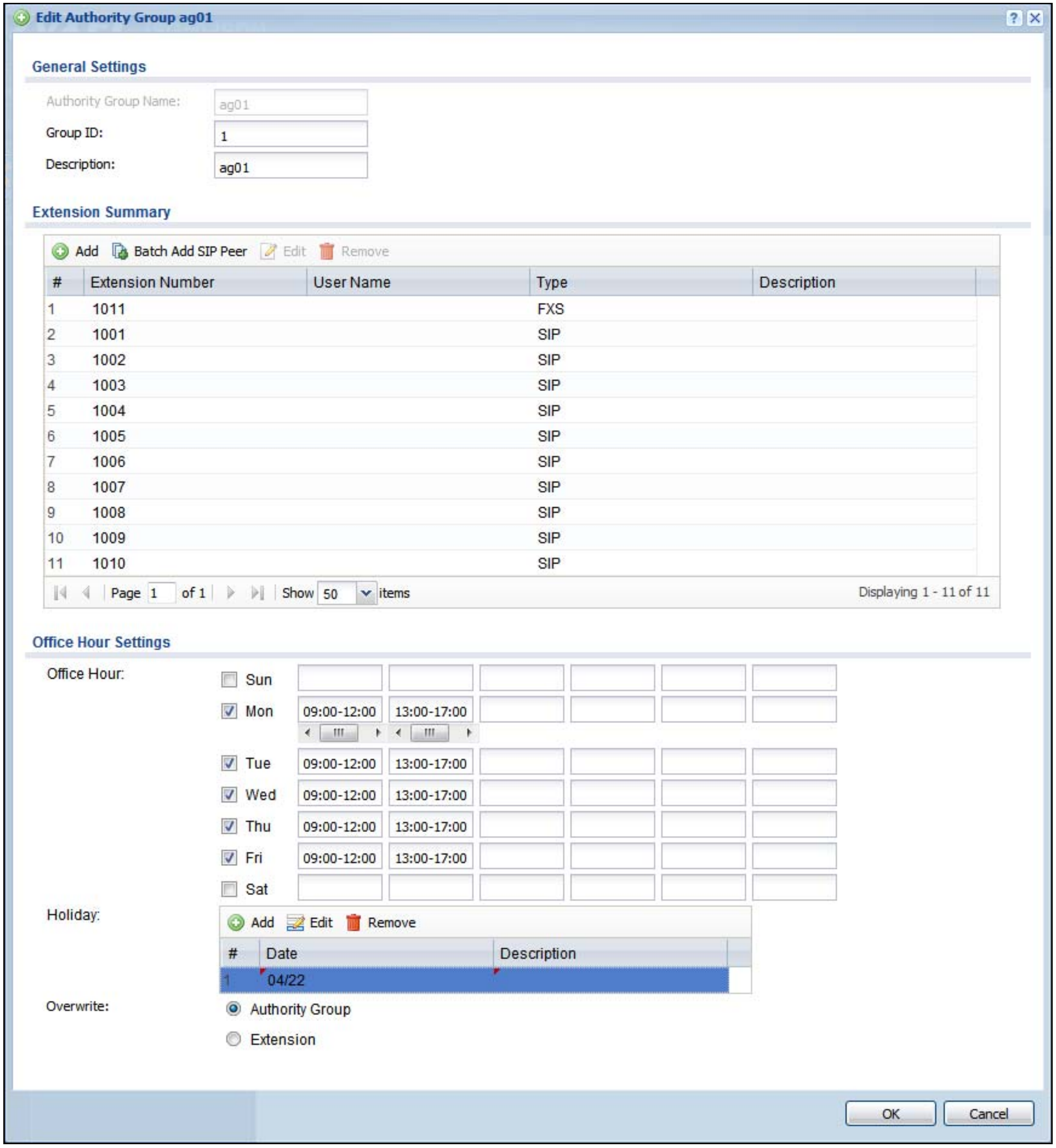
LABEL	DESCRIPTION
Authority Group Name	Type a new name or modify an existing name for this authority group. You can use 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Group ID	Type 1-5 digits to use as an ID for this authority group.
Description	Type a brief description for this authority group. You can use 0-63 alphanumeric characters (A-Z, a-z, 0-9) and spaces. 0 means this field can be left blank.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.2.2 The Authority Group Edit Screen

Use this screen to manage extensions in the authority groups. In the **Authority Group** screen, double-click an authority group entry or select it and click **Edit** to open a screen where you can modify the entry’s settings and manage it’s extensions.

Note: You can use a subscription to increase the number of supported extensions. See Chapter 11 on page 229.

Figure 296 Authority Group Edit



Edit Authority Group ag01

General Settings

Authority Group Name: ag01

Group ID: 1

Description: ag01

Extension Summary

#	Extension Number	User Name	Type	Description
1	1011		FXS	
2	1001		SIP	
3	1002		SIP	
4	1003		SIP	
5	1004		SIP	
6	1005		SIP	
7	1006		SIP	
8	1007		SIP	
9	1008		SIP	
10	1009		SIP	
11	1010		SIP	

Page 1 of 1 Show 50 items Displaying 1 - 11 of 11

Office Hour Settings

Office Hour:

☐	Sun						
☑	Mon	09:00-12:00	13:00-17:00				
☑	Tue	09:00-12:00	13:00-17:00				
☑	Wed	09:00-12:00	13:00-17:00				
☑	Thu	09:00-12:00	13:00-17:00				
☑	Fri	09:00-12:00	13:00-17:00				
☐	Sat						

Holiday:

#	Date	Description
1	04/22	

Overwrite:

● Authority Group

○ Extension

Each field is described in the following table.

Table 154 Authority Group Edit

LABEL	DESCRIPTION
Authority Group Name	This field displays the name of the authority group you are configuring.
Group ID	Type 1-5 digits to use as an ID for this authority group.
Description	Type a brief description for this authority group. You can use 0-63 alphanumeric characters (A-Z, a-z, 0-9) and spaces. 0 means this field can be left blank.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.

Table 154 Authority Group Edit (continued)

LABEL	DESCRIPTION
Batch Add SIP Peer	Click **Batch Add** if you want to configure multiple extensions for IP phones connected to the ISG50.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the extension's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Extension Number	This field displays the extension number.
User Name	This is the username associated with an extension for SIP authentication.
Type	This field displays **SIP**, if this extension is a SIP account. This field displays **FXS**, if this extension is associated with an analog phone connected to an FXS port on the ISG50.
Description	This field displays the description given to this extension.
Office Hour Settings	Use this section to specify office hours on the ISG50.
Sun ~ Sat	Select the days of the week which you want the ISG50 to treat as working days. Specify the time range during the working days that you want the ISG50 to treat as working hours. When entering a time range, the following conditions apply: • You can enter up to six time ranges, with each range consisting of a start time and an end time. • The time entered in each field must be in 24 hour format (such as "08:00" for 8 AM or "13:00" for 1 PM). • The start and end times must be separated by a hyphen.
Holiday	This section allows you to set a specific day of the year as a holiday, which the ISG50 will then treat as "after office hours".
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Date	Enter a date in mm/dd format (double digit month / day; for example, 02/09 for February 9th.)
Description	Enter a description of the holiday using up to 63 alphanumeric characters (A-Z, a-z, 0-9) and spaces.
Overwrite	Select **Authority Group** to apply the current system office hours to this authority group or **Extension** to apply the current system office hours to all extensions.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.3 Extension Features

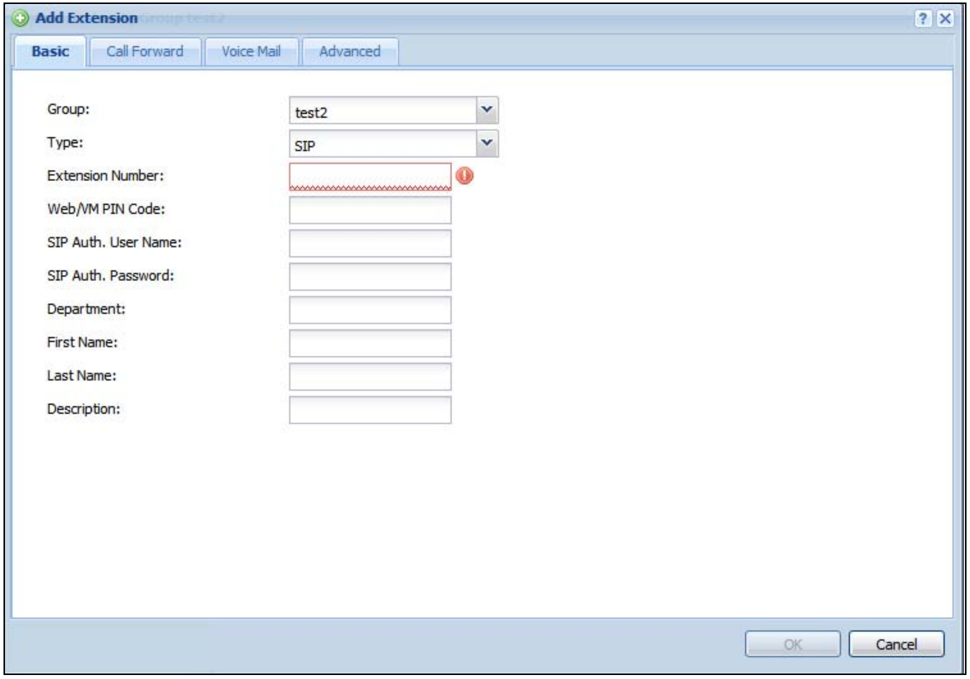
You can configure the following features on a per extension basis:

- **Call Forwarding** - set up call forwarding rules for the individual extension based on the following criteria:
  - Your extension is busy.
  - You turn on DND (Do Not Disturb). You can set up a list of telephone numbers, referred to as the **White List** that ignore DND.
  - Unconditionally, forwards all calls to a specific extension or your voice mail.
  - There is no answer at your extension. This also allows you to set up a **Find Me List**, which is a list of phone numbers where you might be located.
- **Call Blocking** - set up a list of telephone numbers that you don't want to receive calls from. Or, stop calls without caller ID from reaching your extension.
- **Voice Mail Forwarding** - Configure the ISG50 to forward your voice mail messages to your email account.

29.3.1 Extension Add/Edit the Basic Screen

Use this screen to add or edit an extension for an authority group on the ISG50. To access this screen, click the **Add** or **Edit** icon in the **Authority Group Edit** screen.

Figure 297 Extension Add/Edit: Basic



Group: test2
Type: SIP

Each field is described in the following table.

Table 155 Extension Add/Edit: Basic

LABEL	DESCRIPTION
Group	Select the authority group you want this extension to belong to.
Type	Select **SIP** to create a SIP account or **FXS** to configure an extension associated with an analog phone connected to an ISG50 FXS port. This is configurable when adding an extension. If you have already configured the maximum number of a particular type of extension, that type does not display as an option. The rest of the fields in this screen vary based on the interface type.
FXS Interface	Select the port upon which to configure the FXS interface.

Table 155 Extension Add/Edit: Basic (continued)

LABEL	DESCRIPTION
Extension Number	Type the extension number for this IP phone extension. The extension number can be 3-10 digits. This is configurable when adding an extension.
Web/VM PIN Code	Type the 3-10 digit PIN code that allows the person with this extension to access the web portal or Voice Mail.
SIP Auth. User Name	Type the SIP user name associated with this extension. The IP phone registering with the ISG50 must provide this for authentication. The user name can be 1-20 alphanumeric characters (A-Z, a-z, 0-9).
SIP Auth. Password	Select **Customization** and type the SIP password associated with this extension. The IP phone registering with the ISG50 must provide this for authentication. The password can be 3-32 alphanumeric characters (A-Z, a-z, 0-9). Spaces are not allowed.
Department	Type the department for this SIP extension. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
First Name	Type the first name of the person this SIP extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Last Name	Type the last name of the person this SIP extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Description	Type a brief description for this SIP extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9) and spaces. 0 means the field can be left blank.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

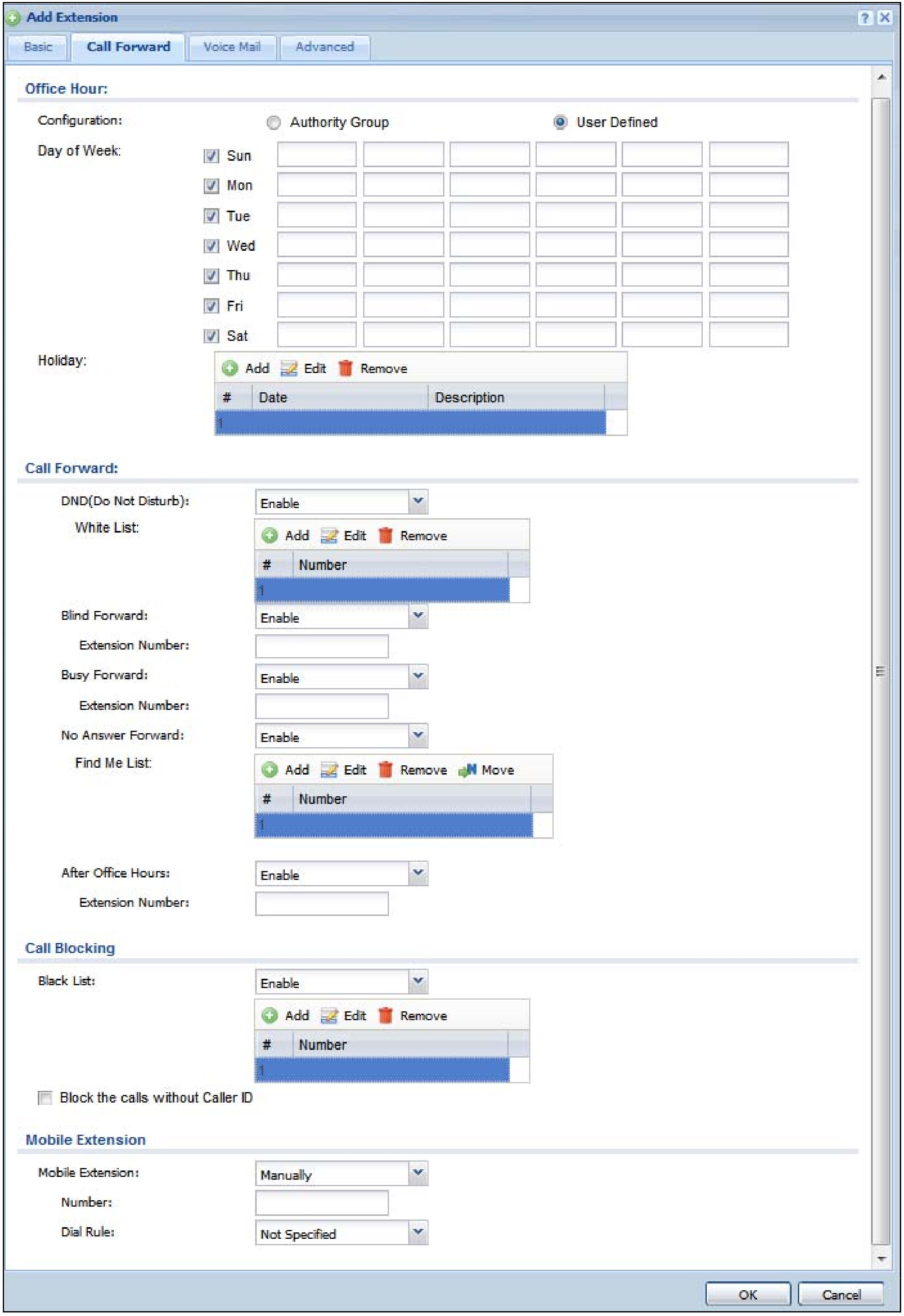
29.3.2 The Extension Call Forward Screen

Use this screen to set up call forwarding and call blocking rules for an extension.

Note: The ISG50 checks any Auto-Attendant call forwarding (see Chapter 31 on page 503) and call blocking (see Section 34.8 on page 542) settings before applying any of the rules created for individual extensions.

To access this screen, click the **Call Forward** tab in any of the SIP extension configuration screens.

Figure 298 Extension Add/Edit: Call Forward


Add Extension
Basic
Call Forward
Voice Mail
Advanced
Add
Edit
Remove
Move
#
Date
Description
Number
OK
Cancel

Office Hour:

Configuration: ○ Authority Group ● User Defined

Day of Week: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Holiday:

Call Forward:

DND(Do Not Disturb): Enable

White List:

Blind Forward: Enable

Extension Number:

Busy Forward: Enable

Extension Number:

No Answer Forward: Enable

Find Me List:

After Office Hours: Enable

Extension Number:

Call Blocking

Black List: Enable

☐ Block the calls without Caller ID

Mobile Extension

Mobile Extension: Manually

Number:

Dial Rule: Not Specified

Each field is described in the following table.

Table 156 Extension Add/Edit: Call Forward

LABEL	DESCRIPTION
Office Hour	The ISG50 has separate rules for call forwarding during office hours than after office hours. The settings you configure specify the office hours for this extension and affect call forwarding during those office hours. If a call is first handled by auto-attendant then it checks the system office hours settings first (and applies any forwarding rules), before checking the office hours configured in this screen.
Configuration	Select **Authority Group** to have the extension use the office hours defined for the authority group to which it belongs. Select **User Defined** to specify custom office hours for this extension.
Day of Week	Select the days of the week which you want the ISG50 to treat as working days. Specify the time range during the working days that you want the ISG50 to treat as working hours. When entering a time range, the following conditions apply: • You can enter up to six time ranges, with each range consisting of a start time and an end time. • The time entered in each field must be in 24 hour format (such as “08:00” for 8 AM or “13:00” for 1 PM). • The start and end times must be separated by a hyphen.
Holiday	This section allows you to set a specific day of the year as a holiday, which the ISG50 will then treat as “after office hours”.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Date	Enter a date in mm/dd format (double digit month / day; for example, 02/09 for February 9th.)
Description	Enter a description of the holiday using up to 63 alphanumeric characters (a-z, A-Z, 0-9, spaces, underscores and hyphens allowed).
Call Forward	Use this section to configure call forwarding settings for the extension.
DND (Do Not Disturb)	Select **Disable** to turn this feature off for this extension. Select **Enable** and the ISG50 will not forward calls to your extension. Use the **White List** to configure telephone numbers which ignore whether you have DND turned on or off. Use the **Add**, **Edit**, and **Remove** icons to create, modify, or delete entries. Select **Voice Mail** and the ISG50 will forward calls directly to voice mail.
Blind Forward	Select **Disable** to turn this feature off for this extension. Select **Enable** and specify an extension or other phone number 3-20 digits in length. The ISG50 will forward all incoming calls to that extension. Select **Voice Mail** and the ISG50 will forward calls directly to voice mail.
Busy Forward	Select **Disable** to turn this feature off for this extension. Select **Enable** and specify an extension or other phone number 3-20 digits in length to forward all incoming calls to that extension when the phone is off the hook. For FXS (analog phones) extensions incoming calls are put into a call waiting queue. Select **Voice Mail** to forward calls directly to voice mail.

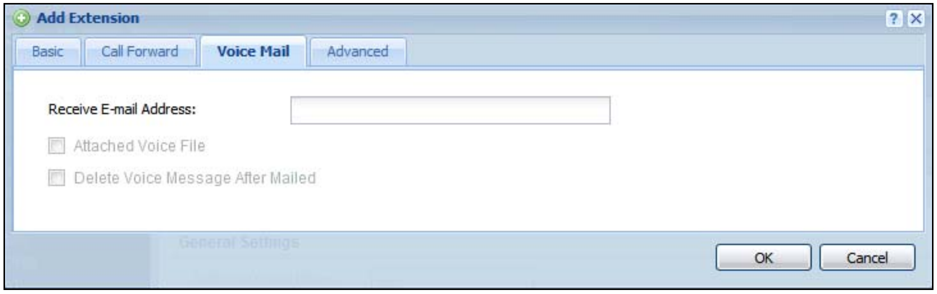
Table 156 Extension Add/Edit: Call Forward (continued)

LABEL	DESCRIPTION
No Answer Forward	Select **Disable** to turn this feature off for this extension. Select **Enable** to forward all incoming calls to the extensions specified in the **Find Me List** when this extension is not answered within the default ring time. Use the **Add**, **Edit**, and **Remove** icons to create, modify, or delete **Find Me List** entries. Select **Voice Mail** to forward calls directly to voice mail.
After Office Hours	These fields specify how to treat calls to your extension that occur after office hours. Select **Disable** to turn this feature off for this extension. Select **Enable** and specify an extension or other phone number 3-20 digits in length. The ISG50 will forward all incoming calls to that extension. Select **Voice Mail** to forward calls directly to voice mail.
Call Blocking	Use this section to configure call blocking settings for the extension.
Black List	Select **Disable** to turn this feature off for this extension. Select **Enable** and the ISG50 will block all incoming calls from extensions that you specify as blacklisted. Use the **Black List** to configure phone numbers that you want to block from calling you. Use the **Add**, **Edit**, and **Remove** icons to create, modify, or delete entries.
Block the calls without Caller ID	Select **Enable** and the ISG50 will block all incoming calls from phone that do not send caller ID.
Mobile Extension	Use this section to configure your mobile extension settings.
Mobile Extension	Select **Manually** to allow authority group members to turn this feature on and off using feature codes. Select **Force Enable** to override the authority group member settings and require all calls to use this feature. For more information on feature codes, see Section 27.3 on page 433.
Number	Enter the number to which you want the ISG50 to forward any incoming calls to your extension.
Dial Rule	Select a dial rule to be applied to the mobile extension. Dial rules correspond to the Least Cost Routing rules used in **Configuration > PBX > Outbound Line Management > LCR**. For more information, see Chapter 32 on page 519. Note: This option only works with digital outbound connections such as BRI. Analog outbound connections such as FXO cannot use this option.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.3.3 The Extension Voice Mail Settings Screen

Use this screen to configure voice mail settings for this extension. To access this screen, click the **Voice Mail** tab in any of the SIP extension configuration screens.

Figure 299 Extension Add/Edit: Voice Mail


Add Extension
Basic
Call Forward
Voice Mail
Advanced
Receive E-mail Address:
☐ Attached Voice File
☐ Delete Voice Message After Mailed
OK
Cancel

Each field is described in the following table.

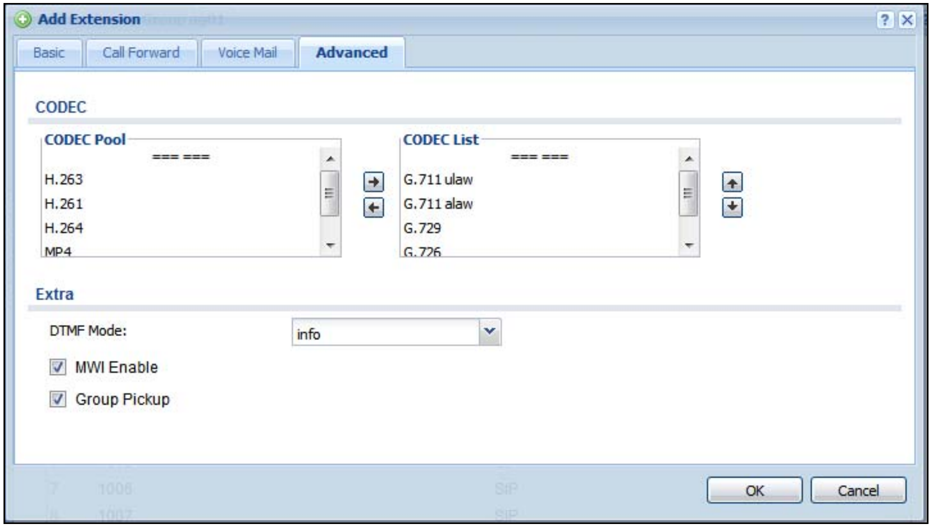
Table 157 Extension Add/Edit: Voice Mail

LABEL	DESCRIPTION
Received E-mail Address	Specify the email address you want to forward your voice message notifications to. If you select the **Attached Voice File** option, then complete voice messages are sent to this email address.
Attached Voice File	Select this feature if you want complete voice messages to be sent to the email address you specified in the **Received E-mail Address** field.
Delete Voice Message After Mailed	Select this box to delete voice mail messages stored on the ISG50 after they have been emailed.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.3.4 The Extension Advanced Screen

Use this screen to configure advanced settings for this extension. The fields available varies depending on the extension type. Click the **Advanced** tab in any of the SIP extension configuration screens to view the screen as shown.

Figure 300 Extension Add/Edit: Advanced



DTMF Mode: info

☑ MWI Enable

☑ Group Pickup

Each field is described in the following table.

Table 158 Extension Add/Edit: Advanced

LABEL	DESCRIPTION
Codec	Select the types of voice coder/decoder (codec) that you want this extension to support when communicating with the ISG50. This is configurable for a SIP extension. The following codecs (shown in highest quality to lowest quality order) are supported by the ISG50: • **G.711 alaw** (typically used in Europe) • **G.711 ulaw** (typically used in North America and Japan) • **G.729** • **G.722** • **G.723.1** • **G.726** See Voice Codecs on page 475 for more information. When two SIP devices start a SIP session, they must agree on a codec. If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The ISG50 allows the following video codecs to pass through: • **H.261** • **H.263** • **H.264** • **MP4** See Video Codecs on page 475 for more information.
Codec Pool	This column indicates the codec types not used by this extension. You can add a codec type to be used by this extension by double-clicking it or highlighting it and hitting the **Right** button.

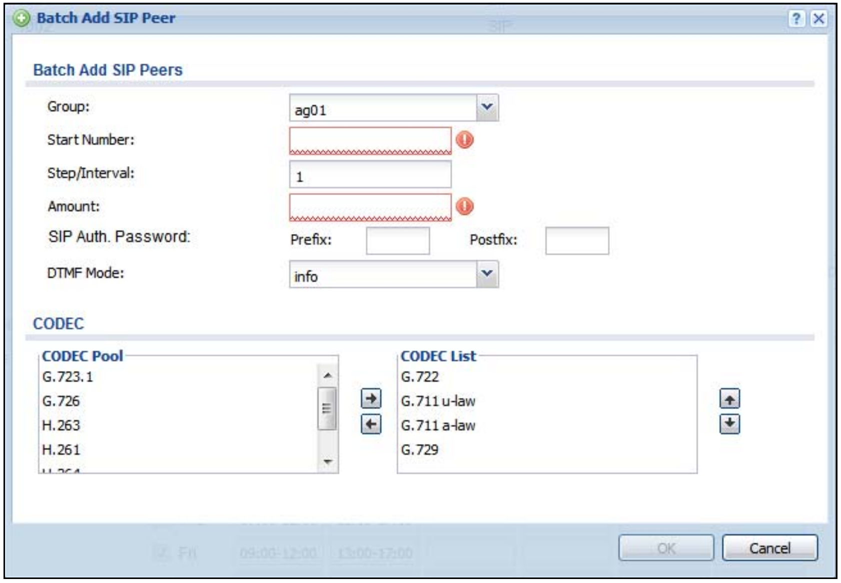
Table 158 Extension Add/Edit: Advanced (continued)

LABEL	DESCRIPTION
Codec List	This column indicates the codec types used by this extension. You can organize the priority of the codecs by highlighting it and clicking the **Up** or **Down** buttons to move the codec higher or lower in priority. The SIP extension attempts to use the higher priority codecs first and tries the lower priority codecs next. You can remove a codec type from being used from this extension by double-clicking it or highlighting it and hitting the **Left** button.
Extra	
DTMF Mode	Control how the ISG50 handles the tones that the IP phone using this extension makes when you push its buttons. This is configurable for a SIP extension. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are: • **rfc2833** - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • **inband** - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. • **info** - Send the DTMF tones in SIP messages.
MWI Enable	Check this box to enable Message Waiting Indicator (MWI) mode for this extension. The ISG50 sends a beeping tone to the IP phone when there is at least one voicemail for this extension.
Group Pickup	Select this to allow other extensions in the authority group with group pickup enabled to answer calls coming into this extension and allow this extension to answer calls coming in for any of the authority group’s extensions that have group pickup enabled. All of an authority group’s extensions that have group pickup enabled ring when a call comes in for any one of them.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.3.5 The Batch Add SIP Screen

Use this screen to configure a range of extensions for IP phones on your network. To access this screen, click the **Batch Add** button in the **Authority Group Edit** screen.

Figure 301 Batch Add SIP Extensions



Group: ag01
Start Number:
Step/Interval: 1
Amount:
SIP Auth. Password: Prefix: Postfix:
DTMF Mode: info

Each field is described in the following table.

Table 159 Batch Add SIP Extensions

LABEL	DESCRIPTION
Batch Add SIP Peers	
Group	Select the authority group you want these extensions to belong to.
Start Number	Type the first extension number for this range of extensions. Extensions can be 3-10 digits long.
Step/Interval	Type the value of the increment, which the ISG50 uses to create this range of extensions.
Amount	Type the number of extensions you want to create. The number of extensions you can create is limited by the subscription service registered on the ISG50 (see Chapter 11 on page 229).
SIP Auth. Password	When you create multiple SIP extensions, you automatically create SIP accounts on the ISG50. The user names for these SIP accounts are the extension numbers. The passwords for the SIP accounts are also the extension numbers. To make the passwords more secure you can add a prefix or a postfix to these extensions. For example type "1" in the **Prefix** field and the SIP account passwords for the SIP extensions you create become "1 + extension number". You can enter up to three letters, numbers or a combination of letters and numbers in the **Prefix** and **Postfix** fields.
DTMF Mode	Control how the ISG50 handles the tones that the IP phones using these extensions make when they push their buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are: • **rfc2833** - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • **inband** - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. • **info** - Send the DTMF tones in SIP messages.
Codec	Select the type of voice coder/decoder (codec) that you want this extension to use when communicating with the ISG50. The following codecs are supported by the ISG50: • **G.711 alaw** (typically used in Europe) • **G.711 ulaw** (typically used in North America and Japan) • **G.729** • **G.722** • **G.723.1** • **G.726** See Voice Codecs on page 475 for more information. When two SIP devices start a SIP session, they must agree on a codec. If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The ISG50 allows the following video codecs to pass through: • **H.261** • **H.263** • **H.264** • **MP4** See Video Codecs on page 475 for more information.
Codec Pool	This column indicates the codec types not used by this extension. You can add a codec type to be used by this extension by double-clicking it or highlighting it and hitting the **Right** button.

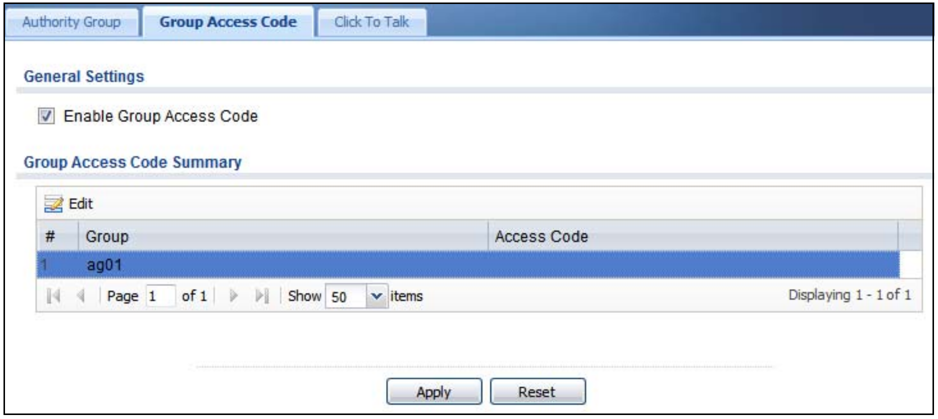
Table 159 Batch Add SIP Extensions (continued)

LABEL	DESCRIPTION
Codec List	This column indicates the codec types used by this extension. You can organize the priority of the codecs by highlighting it and clicking the **Up** or **Down** buttons to move the codec higher or lower in priority. The SIP extension attempts to use the higher priority codecs first and tries the lower priority codecs next. You can remove a codec type from being used from this extension by double-clicking it or highlighting it and hitting the **Left** button.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.4 The Group Access Code Screen

Use this screen to manage the access codes for authority groups on the ISG50. To access this screen, click **Configuration > PBX > Extension Management > Group Access Code**.

Figure 302 Configuration > PBX > Extension Management > Group Access Code



☑ Enable Group Access Code

#	Group	Access Code
1	ag01	

Each field is described in the following table.

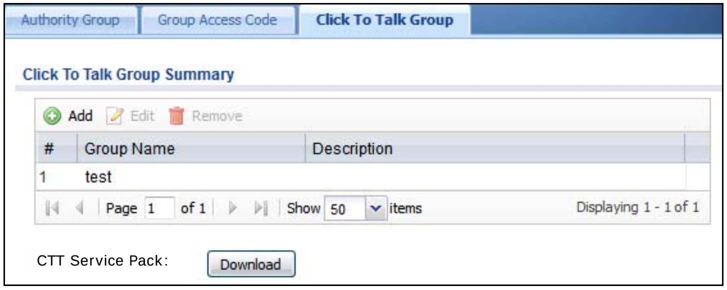
Table 160 Configuration > PBX > Extension Management > Group Access Code

LABEL	DESCRIPTION
Enable Group Access Code	Select this to enable the group access code feature.
Edit	Click this to change the access code for an authority group.
#	This field is a sequential value, and it is not associated with a specific entry.
Group	This is the authority group for which you can configure a call access code. You can only create one call access code per authority group.
Access Code	Use this field to view or enter the access code for this authority group.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

29.5 The Click To Talk Group Screen

This screen allows you to set up CTT groups and their associated extensions. A CTT group is not related to an Authority Groups; it is created solely for the purpose of connecting calls placed with the web-based utility on a web page to the related extensions.

Click **Configuration > PBX > Extension Management > Click To Talk Group to open this screen.**


Authority Group
Group Access Code
Click To Talk Group
Click To Talk Group Summary
Add
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
CTT Service Pack:
Download

#	Group Name	Description
1	test	

Figure 303 Configuration > PBX > Extension Management > Click To Talk Group

Each field is described in the following table.

Table 161 Configuration > PBX > Extension Management > Click To Talk Group

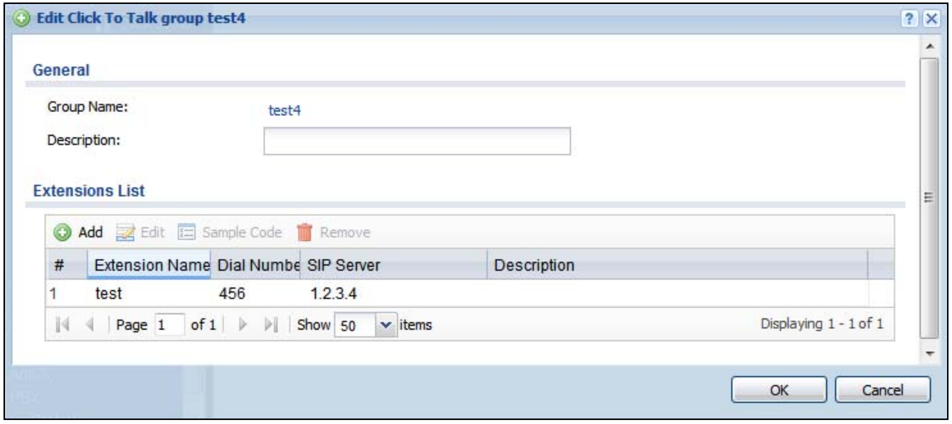
LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Group Name	This indicates the name of the CTT group.
Description	This displays the description associated with the CTT group.
Download	Select a CTT group and click this to download a CTT service pack (ClickToTalk_ISG.cab, clicktotalk.smf, ctt.html, and ctt.js) for embedding the ZyXEL web-based IP phone client in a web page for calling the CTT group.

29.5.1 Add or Edit a Click To Talk Group

Use this screen to create or edit a CTT group.

Click the **Add** or **Edit** icon in the **Click To Talk Group** screen to display the options as shown next.

Figure 304 Click To Talk Group Settings



Group Name: test4

Description:

#	Extension Name	Dial Numbe	SIP Server	Description
1	test	456	1.2.3.4	

Each field is described in the following table.

Table 162 Click To Talk Group Settings

LABEL	DESCRIPTION
Group Name	Enter a name for this CTT group, using up to 20 alphanumeric characters (a-z, A-Z, 0-9); underscores (_) are allowed while spaces and hyphens are not. This is configurable when adding a CTT group.
Description	Enter a description for this CTT group, using up to 63 alphanumeric characters (a-z, A-Z, 0-9).
Extensions List	This section lists the extensions that belong to this CTT group.
Add	Click this to add an extension to this CTT list.
Edit	Click this to edit the selected entry.
Sample Code	When you are in the edit screen, select a CTT extension and click **Sample Code** to generate code which you can use for embedding the ZyXEL web-based IP phone client in a web page for calling the extension.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Extension Name	When you **Add** a new extension, enter the name for this item in the Click To Talk Group Extensions list. When you **Edit** an existing extension, this field displays the name of the extension and cannot be changed.
Dial Number	This indicates the extension associated with this CTT item. This extension must correspond to an existing authority group extension and the dialed number should be authorized in **Group Management**. For more information on extensions and authority groups, see Chapter 33 on page 526.
SIP Server	Use this field to view or edit the address of the SIP server this CTT group is to use.
Description	Use this field to view or edit the description associated with this CTT extension.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

29.5.1.1 Sample HTML for a Click-To-Talk Extension

This is the basic JavaScript and HTML code used to embed the ZyXEL web-based IP phone client in a web page.

```
<script lang="JavaScript" src="http://WEB_SERVER_ADDR/ctt.js"></script>
<a href=
"javascript:Click_to_Talk('WEB_SERVER_ADDR','dicompjrwmA7352)yshvpdqg@wm4rV
q[8&yuhvuhgrhx?zo3qTpZ:(vitvitltcghr@595246.542344<5483*fwqfpsfhA5)uuhvkgAL
olcqr(wynqinlt?474165173.533*vxrnhprrvv@82')">Click_to_Talk</a>
```

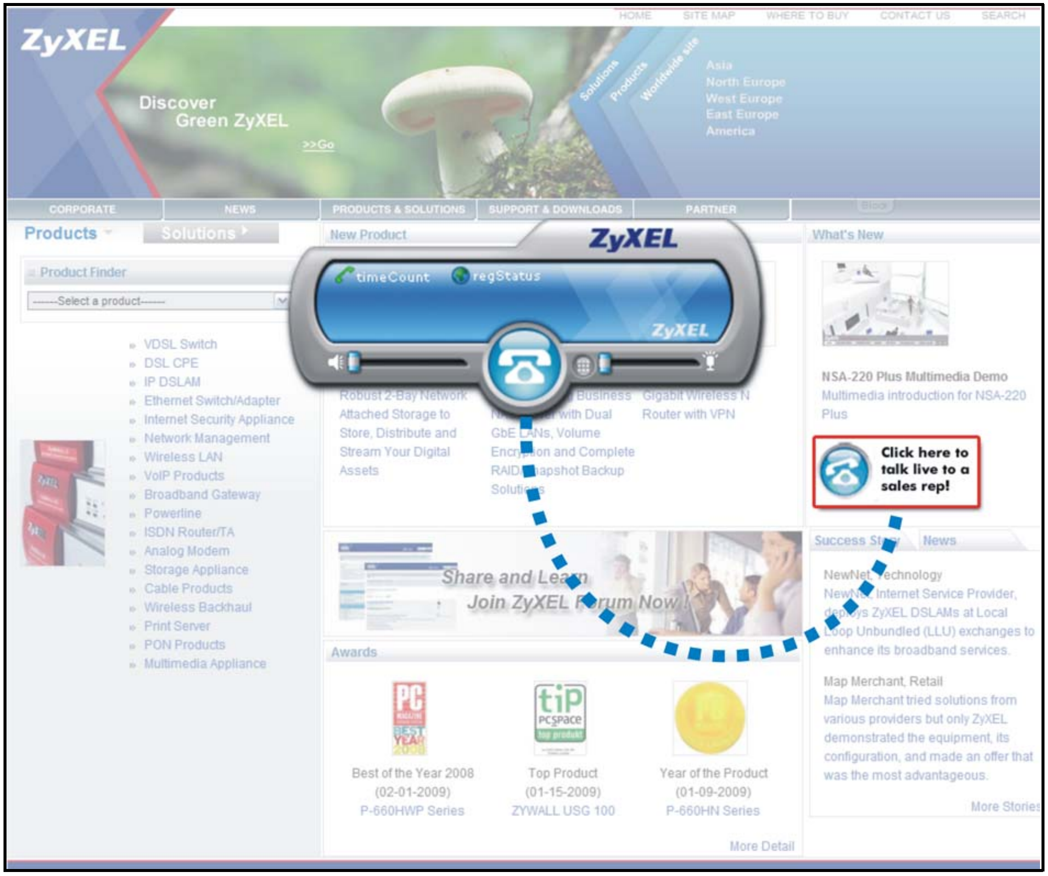
Note: You must replace both `WEB_SERVER_ADDR` strings in the sample code with your own company’s website. For example, “www.zyxel.com”.

Note: If you change your dial number or WAN IP address, then you must regenerate the sample code.

Note: Makes sure the following four files are in a single location: ctt.js, ctt.html, clicktotalk.cab and clicktotalk.swf.

Once you embed the link, a visitor to your website can then click it and open the web-based IP phone to speak directly to person at the other end.

Figure 305 Sample CTT Web Page


ZyXEL
Discover
Green ZyXEL
CORPORATE
NEWS
PRODUCTS & SOLUTIONS
SUPPORT & DOWNLOADS
PARTNER
Products
Solutions
Product Finder
New Product
What's New
timeCount
regStatus
ZyXEL
NSA-220 Plus Multimedia Demo
Click here to talk live to a sales rep!
Share and Learn
Join ZyXEL Forum Now!
Success Story
News
Awards
Best of the Year 2008
Top Product
Year of the Product
More Detail
More Stories

29.6 Authority Group Technical Reference

This section contains technical background information about the **Authority Group** screens.

Voice Codecs

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The following table describes the codecs supported on the ISG50

Table 163 Voice Codecs Supported

CODEC	DESCRIPTION
G.711	This is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization "reads" the analog signal and then "writes" it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as "quantization noise"). G.711 provides excellent sound quality but requires 64kbps of bandwidth. There are two main algorithms defined in the G.711 standard, the µ-law algorithm (used in North America & Japan) and a-law algorithm (used in Europe and the rest of the world).
G.722	G.722 is an ADPCM codec (see G.726) working at 48 ~ 64 Kbps, with an audio sample rate of 16 KHz. G.722 provides excellent sound quality.
G.723.1	This is an ITU (International Telecommunication Union) standard for voice coding. The G.723.1 codec compresses voice audio in 30 ms frames. The G.723.1 operates at two bitrates: 6.3 kbps when sampling at 24 bytes or 5.3 kbps when sampling at 20 bytes per 30 ms frame.
G.726	This is an Adaptive Differential Pulse Code Modulation (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. G.726 operates at 16, 24, 32 or 40 kbps. Differential (or Delta) PCM is similar to PCM, but encodes the audio signal based on the difference between one sample and a prediction based on previous samples, rather than encoding the sample’s actual quantized value. Many thousands of samples are taken each second, and the differences between consecutive samples are usually quite small, so this saves space and reduces the bandwidth necessary.
G.729	This is an Analysis-by-Synthesis (AbS) hybrid waveform codec. It uses a filter based on information about how the human vocal tract produces sounds. The codec analyzes the incoming voice signal and attempts to synthesize it using its list of voice elements. It tests the synthesized signal against the original and, if it is acceptable, transmits details of the voice elements it used to make the synthesis. Because the codec at the receiving end has the same list, it can exactly recreate the synthesized audio signal. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

Video Codecs

Video codecs are used by video phones to compress the amount of information sent between two devices. Video codecs encode video signals into digital signals and decode the digital signals back into video signals. Although the ISG50 does not perform any video coding, it does support the pass through of the following video codecs.

Table 164 Video Codecs Supported

CODEC	DESCRIPTION
H.261	This is an ITU (International Telecommunication Union) video coding standard. H.261 was designed in 1990 and is considered the first practical video coding standard. The data rate of the coding algorithm is able to operate between 40 kbps and 2 Mbps. H.261 was targeted primarily to work over circuit-switched networks and has since been superseded by more efficient video coding standards.
H.263	This video codec is based closely on the H.261 standard, but as a general rule requires half the bandwidth to achieve the same quality video. H.263 is capable of streaming video at bandwidths as low as 20 kbps to 24 kbps.
H.264	This video codec is video compression technology that falls under the MPEG-4 standard, also known as MPEG-4 Part 10. H.264 can provide excellent video quality at bandwidth from 40 Kbps upwards.
MP4	MPEG-4 is an audio/video compression technology developed by the Motion Picture Experts Group. You need to enable MPEG-4 if you want SIP phones to make video calls via the ISG50.

30

Outbound Trunk Group

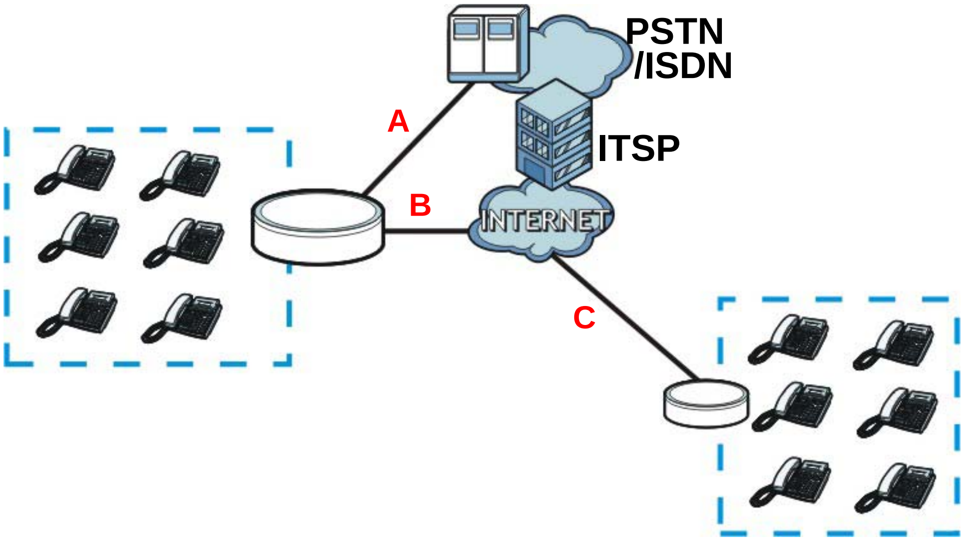
30.1 Overview

This covers you how to manage outside lines on the ISG50.

The following diagram shows the ISG50 connected to the various types of outside connections:

- FXO/BRI Trunk (**A**): shows the ISG50 connected to the PSTN (Public Switched Telephone Network) or ISDN (Integrated Service Digital Network) via an FXO/BRI port on the ISG50. You can also use the FXO ports to connect to a traditional analog PBX or use the BRI port to connect to a basic rate interface, if your organization has one.
- SIP Trunk (**B**): shows the ISG50 connected to a SIP gateway at your VoIP service provider (ITSP: Internet Telephony Service Provider). You can use the SIP trunk to connect to a SIP gateway on which you have an existing SIP account.
- Trusted Peer (**C**): shows the ISG50 connected to another ISG50 (for example, at your branch office). You can establish a trusted peer connection with another SIP server that lists your ISG50 as a trusted peer.

Figure 306 Outbound Line Overview



30.1.1 What You Can Do in this Chapter

- Use the **Outbound Trunk Group** screens (starting in Section 30.2 on page 481) to manage the outside lines on the ISG50.
- Use the **Auto-Attendant** screens (starting in Section 31.2 on page 505) to configure the default and customized auto-attendants the ISG50 uses.

- Use the **LCR** screens (starting in Section 31.2 on page 505) to configure the Configure Least Cost Routing (LCR) dialing rules.

30.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Outbound Trunk

The outbound lines define a connection between the ISG50 and the PSTN, ISDN, ITSP or your trusted peer (another ISG50). To make calls from extensions on your network you still have to define LCRs, which are outbound dialing rules (See Chapter 32 on page 519). You also have to configure an auto-attendant to handle the forwarding of incoming calls (See Chapter 31 on page 503).

FXO Trunk

FXO trunks allow you to connect to the PSTN (through your traditional analog telephone service provider) or a traditional analog PBX in your organization.

BRI Trunk

BRI trunks allow you to connect to the ISDN or an ISDN PBX in your organization.

SIP Trunk

SIP trunks allow you to connect to a VoIP service provider.

Trusted Peer Trunk

Trusted peers refer to connections to another SIP server (for example another ISG50) that has configured your ISG50 as a trusted peer. Your organization may want to use trusted peer connections between remote branch offices.

Using Multiple ISDN Numbers

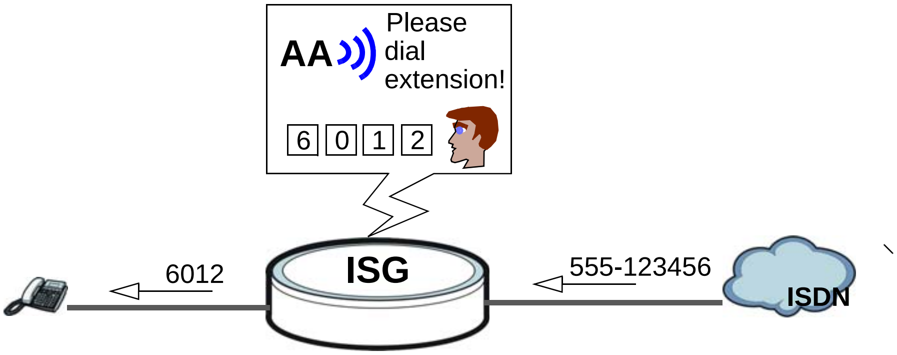
You may have multiple ISDN numbers from your ISDN service provider. You can map these numbers to the AA (Auto Attendant) and directly to extension numbers.

Note: Use AA if you do not have multiple ISDN numbers.

AA (Auto Attendant)

After calling the number, the caller is prompted to dial the extension number.

Figure 307 Auto Attendant (AA) Example

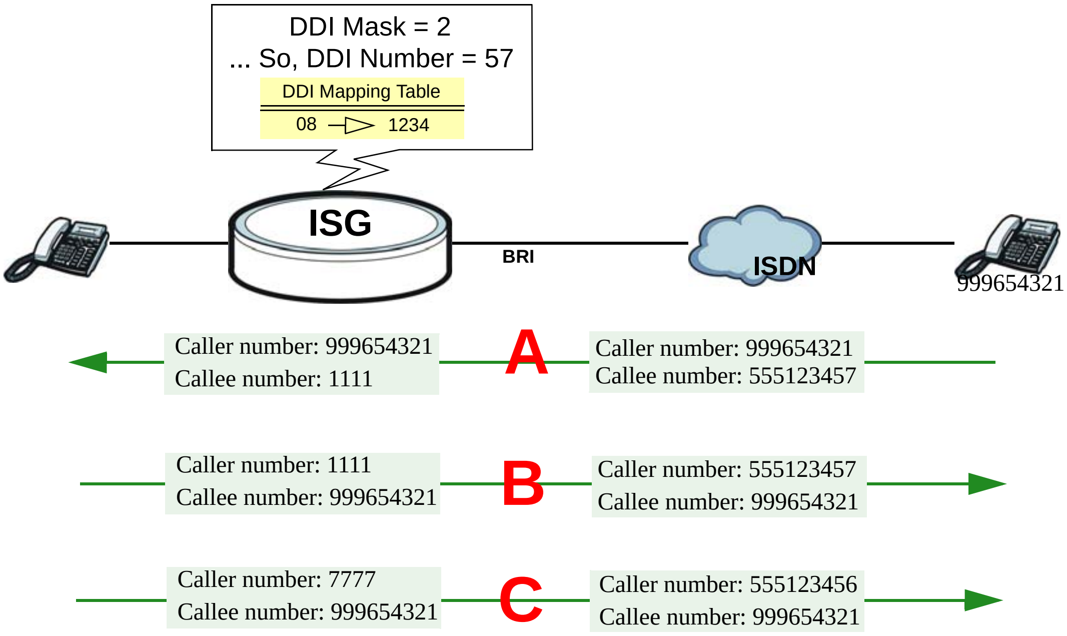

AA
Please dial extension!
6 0 1 2
ISG
6012
555-123456
ISDN

DDI (Direct Dial In)

DDI (also called DID, Direct Inward Dial) is a feature that maps a public number to an extension number. DDI enables a caller to call an extension number without going through an operator. When people give out their contact number and say it's a “direct line”, often what they mean is that it's a DDI number.

For example, your company has 10 phone numbers (555-123456~555-123465). You can choose 555-123456 to be the directory number (the company’s representative phone number) and map the others to extensions using DDI. Define 2 digits (from right to left) for the DDI mask. Associate “**57**” to an extension number (for example, **1111**).

Figure 308 DDI Example


DDI Mask = 2
... So, DDI Number = 57
DDI Mapping Table
08 → 1234
ISG
BRI
ISDN
999654321
Caller number: 999654321
Callee number: 1111
A
Caller number: 999654321
Callee number: 555123457
Caller number: 1111
Callee number: 999654321
B
Caller number: 555123457
Callee number: 999654321
Caller number: 7777
Callee number: 999654321
C
Caller number: 555123456
Callee number: 999654321

This example also shows three call examples.

A - When an outsider calls **555-123457**, the call is mapped to the extension **1111**.

B - When someone makes an outgoing call from the extension **1111**, the caller ID shown to the callee is **555-123457**.

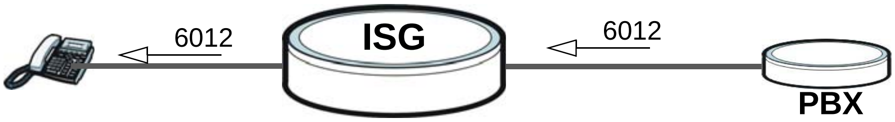
C - When you make a call over this outbound line from an extension that is NOT listed in the DDI mapping table, the directory number (**555123456** in this example) is the number that displays on the callee's caller ID.

Note: Calls on incoming ISDN numbers that are not included in the DDI mapping table go to the AA.

Calling Directly to an Extension

ISDN calls can be made directly to an extension number from another PBX that is connected directly. In this example, all incoming calls are forwarded to the extension called.

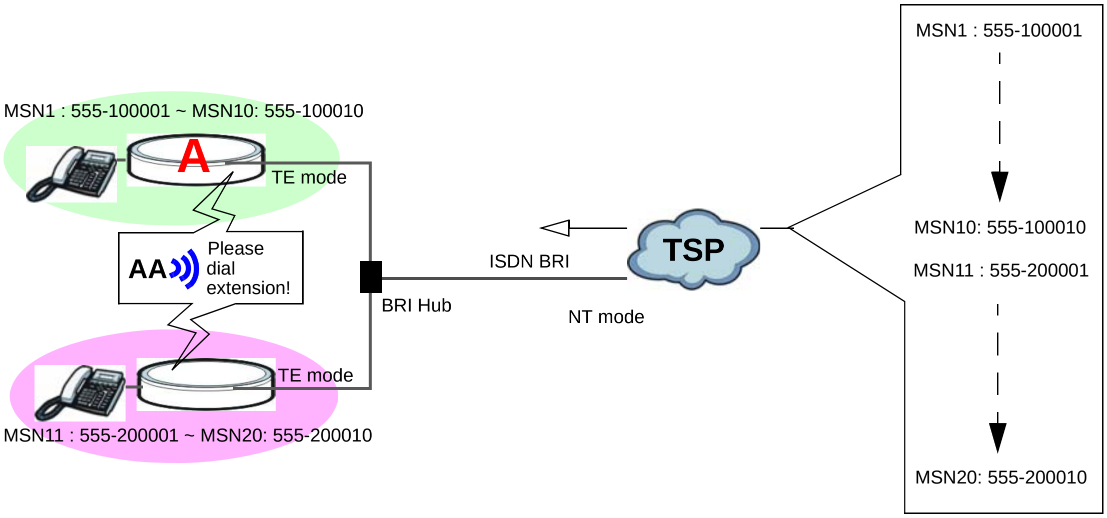
Figure 309 Direct Example


6012
ISG
6012
PBX

MSNs (Multiple Subscriber Numbers)

This feature is relevant to ISDN BRI (TE mode) only. In this example, two ISG50s use a BRI hub to share a single BRI line to one TSP (Telecommunications Service Provider). Each ISG50 can have up to 10 BRI trunks for each BRI line it uses. Each BRI trunk uses a unique MSN. This example uses 20 MSNs for the single BRI line. These MSNs must correspond to those configured on the connected TSP's ISDN device. Device **A**'s auto-attendant system answers the incoming call only when the number matches the MSN configured on device **A**.

Figure 310 MSN Example


MSN1 : 555-100001 ~ MSN10: 555-100010
A
TE mode
AA
Please dial extension!
BRI Hub
ISDN BRI
NT mode
TSP
TE mode
MSN11 : 555-200001 ~ MSN20: 555-200010
MSN1 : 555-100001
MSN10: 555-100010
MSN11 : 555-200001
MSN20: 555-200010

30.1.3 Before You Begin

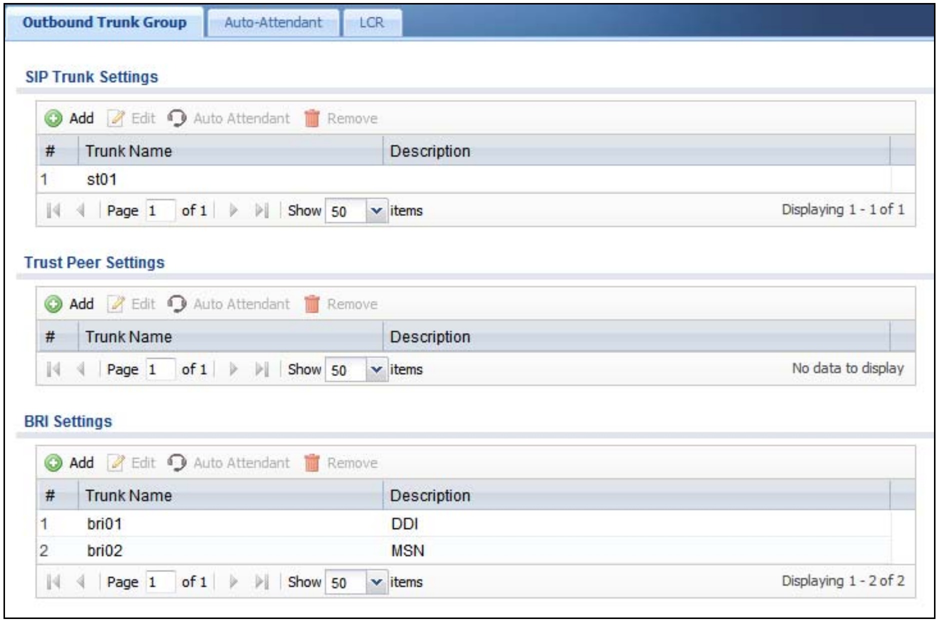
Before you start to configure an outbound line group, please consider the following.

- In order to create an FXO/BRI trunk the ISG50 must have a corresponding FXO or BRI port.
- In order to create a SIP trunk you must already have a SIP account and a network connection to your VoIP service provider.
- In order to create a Trusted Peer trunk you must already have a SIP server's information (for example, IP address) and a network connection to the peer device.

30.2 Outbound Trunk Group Screen

Use this screen to manage the outside lines on the ISG50. To access this screen, click **Configuration > PBX > Outbound Line Management > Outbound Trunk Group.**

Figure 311 Outbound Line Management > Outbound Trunk Group



SIP Trunk Settings

#	Trunk Name	Description
1	st01	

Displaying 1 - 1 of 1

Trust Peer Settings

#	Trunk Name	Description

No data to display

BRI Settings

#	Trunk Name	Description
1	bri01	DDI
2	bri02	MSN

Displaying 1 - 2 of 2

Each field is described in the following table.

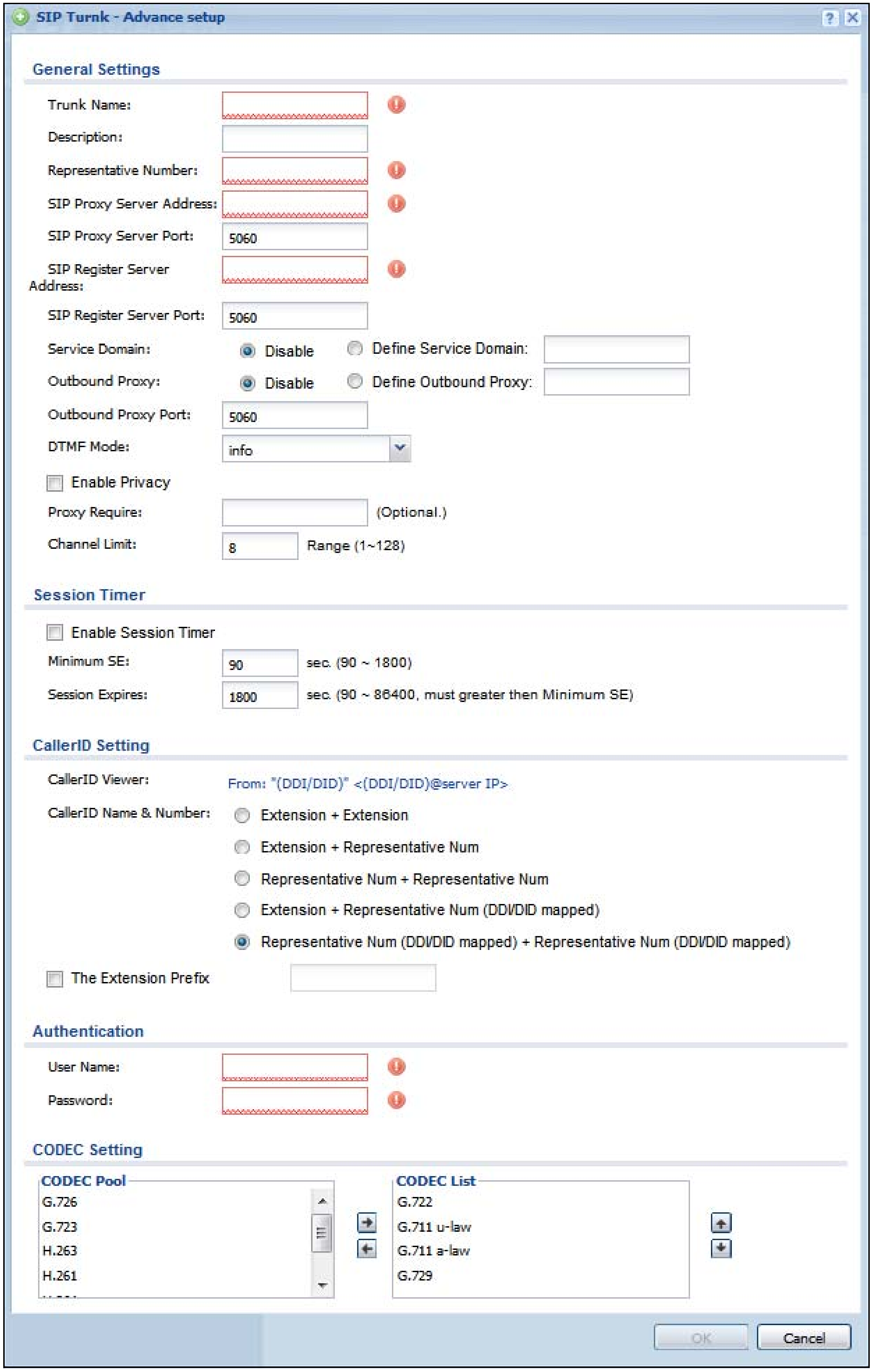
Table 165 Outbound Line Management > Outbound Trunk Group

LABEL	DESCRIPTION
SIP Trunk / Trust Peer / FXO / BRI Settings	These headings divide the screen into sections based on the type of outside line you have configured: • **SIP Trunk** - refers to a connection from the ISG50 to a SIP server at your VoIP service provider. • **Trust Peer** - refers to a connection to another SIP server (for example another ISG50) that has configured your ISG50 as a trusted peer. • **FXO** - refers to a connection from the ISG50 to the PSTN (your local telephone company) via the FXO port on the ISG50. • **BRI** - refers to a connection from the ISG50 to the basic rate ISDN trunk line via the BRI port on the ISG50.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Auto Attendant	Select an entry and click **Auto Attendant** to assign an auto attendant to the outbound line group.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Trunk Name	This field displays the name of an outbound line trunk.
Description	This field displays the description for an outbound line trunk.

30.2.1 SIP Trunk Add/Edit

Use this screen to configure a SIP trunk. Click the **Add** or **Edit** icon in the **SIP Trunk Settings** section of the **Outbound Trunk Group** configuration screen to view the screen as shown.

Figure 312 SIP Trunk Add/Edit



General Settings

Trunk Name:
Description:
Representative Number:
SIP Proxy Server Address:
SIP Proxy Server Port: 5060
SIP Register Server Address:
SIP Register Server Port: 5060
Service Domain: ● Disable ○ Define Service Domain:
Outbound Proxy: ● Disable ○ Define Outbound Proxy:
Outbound Proxy Port: 5060
DTMF Mode: info
☐ Enable Privacy
Proxy Require: (Optional.)
Channel Limit: 8 Range (1~128)

Session Timer

☐ Enable Session Timer
Minimum SE: 90 sec. (90 ~ 1800)
Session Expires: 1800 sec. (90 ~ 86400, must greater then Minimum SE)

CallerID Setting

CallerID Viewer: From: "(DDI/DID)" <(DDI/DID)@server IP>
CallerID Name & Number:
○ Extension + Extension
○ Extension + Representative Num
○ Representative Num + Representative Num
○ Extension + Representative Num (DDI/DID mapped)
● Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)
☐ The Extension Prefix

Authentication

User Name:
Password:

CODEC Setting

CODEC Pool: G.726, G.723, H.263, H.261
CODEC List: G.722, G.711 u-law, G.711 a-law, G.729

Each field is described in the following table.

Table 166 SIP Trunk Add/Edit

LABEL	DESCRIPTION
Trunk Name	Type the name of this SIP trunk. This field can be 1-30 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). The first character must be a letter.
Description	Type the description for this SIP interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Representative Number	Enter the phone number that the called party sees if outgoing calls through this outbound line group don't match configured rules. associated with the SIP account for this SIP trunk. In the full SIP URI, this is the part before the @symbol. You can use 3-40 printable ASCII characters.
SIP Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 64 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Proxy Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Register Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Proxy Server Address** field. You can use up to 64 printable ASCII characters.
SIP Register Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Proxy Server Port** field.
Service Domain	Select **Define Service Domain** and enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 64 printable ASCII Extended set characters. If you choose not to use a service domain, select **Disable**.
Outbound Proxy	**Select Define Outbound Proxy** and enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 64 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. If you choose not to use an outbound proxy server, select **Disable**.
Outbound Proxy Port	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'. If the outbound proxy is disabled, then this port will be ignored.
DTMF Mode	Control how the ISG50 handles the tones that the IP phones on your network make when they push their buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are: • **info** - Send the DTMF tones in SIP messages. • **rfc2833** - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • **inband** - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones.
Enable Privacy	Select this to replace the caller's name and number with "Anonymous". For example, "Anonymous"<Anonymous@172.1.1.253>. Clear this to display caller ID as displayed in this screen's **CallerID Viewer** field.
Proxy Require	Enter this (0~127 alphanumeric characters) to inform the SIP server that this device is behind a firewall or NAT device. Fill this field in only if you were given information by your SIP service provider.
Channel-limit	Specify the maximum number of SIP calls (1~128) allowed to be made through this trunk connection at one time.
Session Timer	
Enable Session Timer	Select this activate the ISG50's session timer. If you encounter connectivity issues with your network or Internet, then it is suggested that you use the session timer.

Table 166 SIP Trunk Add/Edit (continued)

LABEL	DESCRIPTION
Minimum SE	Enter the minimum session expiry time in seconds. The allowable range is 90~1800 seconds. When an incoming call requests a session expiry time that is lower than this, the ISG50 uses this value instead.
Session Expires	Enter the session expiry time in seconds for all phone connections on this trunk. The allowable range is 90~86400 seconds. This value cannot be lower than the **Minimum SE**. This allows the ISG50 to automatically disconnect any phone calls on this trunk after a certain period of inactivity.
CallerID Setting	Configure this section to change the format of identification you want to send when you make VoIP phone calls. The default format is **"From: "Extension"<Extension@Server IP>"**.
CallerID Viewer	This field displays the caller ID format shown to the callees depending on the setting you configure in the **CallerID Name & Number** and **The Extension Prefix** fields.
CallerID Name & Number	Select the caller ID display format to use for the SIP trunk's outgoing calls. A caller ID consists of a call ID name (**A**), a caller ID number (**B**) and a SIP server IP address (**C**). The caller ID has the following format: "**A**"<**B@C**>. The choices are: (In the following examples, we assume a company representative number is 12345678, their SIP server IP is 10.1.1.1, a caller extension number is 1111 and DDI/DID number 12345555 can map to the extension 1111.) • **Extension + Extension**: Displays the caller's extension number in **A** and **B**. For example, "1111"<1111@10.1.1.1>. • **Extension + Representative Num.**: Displays the caller's extension number in **A** and the SIP trunk's representative number in **B**. For example, "1111"<12345678@10.1.1.1>. • **Representative Num. + Representative Num.**: Displays the SIP trunk's representative number in **A** and **B**. For example, "12345678"<12345678@10.1.1.1>. Select this format if you don't want callees to know the caller's extension number. • **Extension + Representative Num (DDI/DID mapped)**: Displays the caller's extension number in **A** and the SIP trunk's DDI/DID mapped representative number in **B**. For example, "1111"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **B**. • **Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)**: Displays the SIP trunk's DDI/DID mapped representative number in both **A** and **B**. For example, "12345555"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **A** and **B**.
The Extension Prefix	Specify whether to add a prefix number in the callerID name when you make calls through this trunk connection. The availability of this setting varies depending on the format of **CallerID Name & Number** you selected. This field can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and pluses (+)
Authentication	
Username	Type the SIP user name associated with this extension. The IP phone registering with the ISG50 must provide this for authentication. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9).
Password	Type the SIP password associated with this extension. The IP phone registering with the ISG50 must provide this for authentication. This field can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), pluses (+), periods (.), and "at" symbols (@).

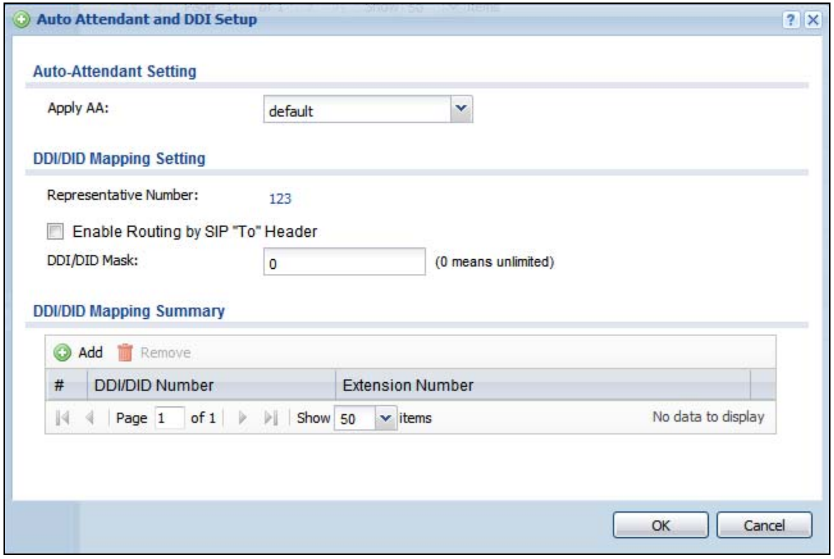
Table 166 SIP Trunk Add/Edit (continued)

LABEL	DESCRIPTION
Codec Setting	Select the type of voice coder/decoder (codec) that you want this extension to use when communicating with the ISG50. The following codecs (shown in highest quality to lowest quality order) are supported by the ISG50: • **G.711 alaw** (typically used in Europe) • **G.711 ulaw** (typically used in North America and Japan) • **G.729** • **G.722** • **G.723.1** • **G.726** See Voice Codecs on page 475 for more information. When two SIP devices start a SIP session, they must agree on a codec. If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The ISG50 allows the following video codecs to pass through: • **H.261** • **H.263** • **H.264** • **MP4** See Video Codecs on page 475 for more information on video codecs.
Codec Pool	This column indicates the codec types not used for these extensions. You can add a codec type to be used for these extensions by highlighting it and clicking the **Right** button.
Codec List	This column indicates the codec types used by these extensions. You can organize the priority of the codecs by highlighting it and clicking the **Up** or **Down** buttons to move the codec higher or lower in priority. The SIP extensions attempt to use the higher priority codecs first and try the lower priority codecs next. You can remove a codec type from being used from these extension by highlighting it and clicking the **Left** button.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

30.2.2 SIP Auto Attendant and DDI Setup

Use this screen to select which auto-attendant should be used with this outbound line group. See Chapter 31 on page 503 for information on configuring auto-attendants. You can also configure your DID (Direct Inward Dialing) settings. In the the **Outbound Trunk Group** configuration screen, select a SIP trunk and click the **Auto-Attendant** icon to view the screen as shown.

Figure 313 SIP Auto Attendant and DDI Setup



Apply AA: default

Representative Number: 123

☐ Enable Routing by SIP "To" Header

DDI/DID Mask: 0 (0 means unlimited)

#	DDI/DID Number	Extension Number

No data to display

Each field is described in the following table.

Table 167 SIP Auto Attendant and DDI Setup

LABEL	DESCRIPTION
Auto-Attendant Setting	
Apply AA	Select an Auto Attendant or ACD skill profile used for the calls incoming through this outbound line trunk. Select **default** to forward all incoming calls on this outbound line group according to each extension’s settings. Select **ACD** if you want to forward all incoming calls on this outbound line group to the group of agents associated with a specific skill name. Select **FAX** if you want to forward all incoming calls on this outbound line group to a fax machine located at a specific extension. Select **Extension** if you want to directly forward all incoming calls through this outbound line group to an extension.
Skill	This field displays if you select **ACD** in the **Apply AA** field. Select the skill name of the agents to associate with this outbound line trunk.
Extension Number for Fax	This field is only available if you select **FAX** in the **Apply AA** field. Type the extension of the fax machine you want to forward calls to.
Extension Number	This field is only available if you select **Extension** in the **Apply AA** field. Type an extension you want to forward calls to.
DDI/DID Mapping Setting	
Representative Number	This field displays the representative number configured for the trunk.

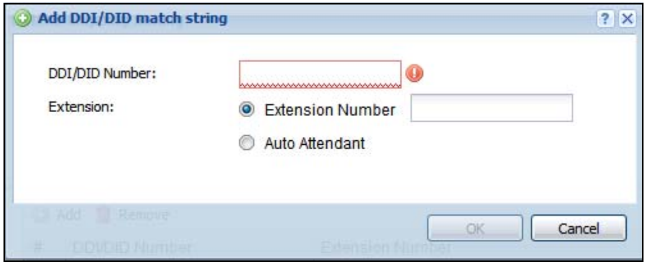
Table 167 SIP Auto Attendant and DDI Setup

LABEL	DESCRIPTION
Enable Routing by SIP "To" Header	Select this if this auto-attendant interacts with a SIP server that uses the SIP To header to do the DDI/DID mapping. If this SIP trunk outbound line group has DDI/DID mode enabled, using this deletes all of the this SIP trunk outbound line group's DDI/DID mapping settings and sets the **DDI/DID Mask** to 0. Clear this to use the SIP request URI to do the DDI/DID mapping.
DDI/DID Mask	Enter a number (0~10) to decide the number of digits you want to enter for the next DDI/DID number(s). 0 means you can enter any number of digits for the next DDI/DID number(s).
DDI/DID Mapping Summary	Use this section to manage the DDI/DID numbers which allow outsiders to call and reach extensions directly.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
DDI/DID Number	This field shows the DDI/DID number outsiders can call to reach the entry's extension directly.
Extension Number	This field shows the extension that outsiders can reach directly by calling the entry's DDI/DID number.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.3 Add DDI/DID Number

Use this screen to add a DDI/DID number for an auto attendant to allow outsiders to call and reach an extension directly. In the auto attendant screen, click the **DDI/DID Mapping Summary**'s **Add** icon to view the screen as shown.

Figure 314 Add DDI/DID Number



Each field is described in the following table.

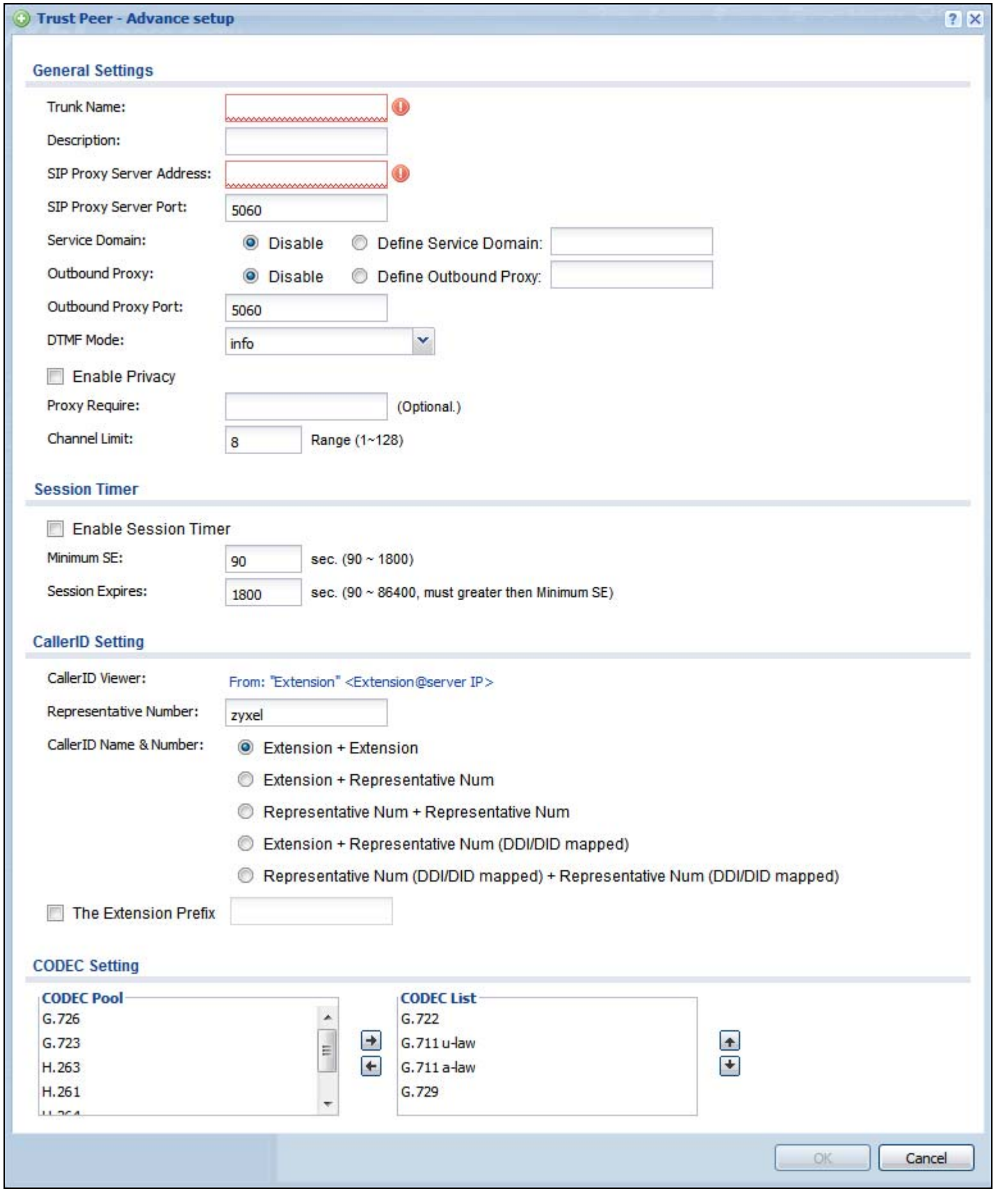
Table 168 Add DDI/DID Number

LABEL	DESCRIPTION
DDI/DID Number	Enter a DDI/DID number which allows outsiders to call and reach an extension directly. The number of digits you can enter in this field depends on what you set in the **Representative Number DDI/DID Mask** field. This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.
Extension	Select **Extension Number** and enter the extension number to which the DDI/DID number maps. This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999. Alternatively, select **Auto-Attendant** to forward the matched DDI calls to auto-attendant.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.4 Trusted Peer Trunk Add/Edit

Use this screen to configure a trusted peer trunk. Click the **Add** or **Edit** icon in the **Trust Peer Settings** section of the **Outbound Trunk Group** configuration screen to view the screen as shown.

Figure 315 Trusted Peer Trunk Add/Edit



Trust Peer - Advance setup

General Settings

Trunk Name:

Description:

SIP Proxy Server Address:

SIP Proxy Server Port: 5060

Service Domain: ● Disable ○ Define Service Domain:

Outbound Proxy: ● Disable ○ Define Outbound Proxy:

Outbound Proxy Port: 5060

DTMF Mode: info

☐ Enable Privacy

Proxy Require: (Optional.)

Channel Limit: 8 Range (1~128)

Session Timer

☐ Enable Session Timer

Minimum SE: 90 sec. (90 ~ 1800)

Session Expires: 1800 sec. (90 ~ 86400, must greater then Minimum SE)

CallerID Setting

CallerID Viewer: From: "Extension" <Extension@server IP>

Representative Number: zyxel

CallerID Name & Number:

● Extension + Extension

○ Extension + Representative Num

○ Representative Num + Representative Num

○ Extension + Representative Num (DDI/DID mapped)

○ Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)

☐ The Extension Prefix

CODEC Setting

CODEC Pool: G.726, G.723, H.263, H.261

CODEC List: G.722, G.711 u-law, G.711 a-law, G.729

Each field is described in the following table.

Table 169 Trusted Peer Trunk Add/Edit

LABEL	DESCRIPTION
Trunk Name	Type the name of this trunk. This field can be 1-30 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). The first character must be a letter.
Description	Type the description for this interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
SIP Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 64 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Proxy Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Service Domain	Select **Define Service Domain** and enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 64 printable ASCII Extended set characters. If you choose not to use a service domain, select **Disable**.
Outbound Proxy	**Select Define Outbound Proxy** and enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 64 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. If you choose not to use an outbound proxy server, select **Disable**.
Outbound Proxy Port	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'. If the outbound proxy is disabled, then this port will be ignored.
DTMF Mode	Control how the ISG50 handles the tones that the IP phones on your network make when they push their buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are: • **info** - Send the DTMF tones in SIP messages. • **rfc2833** - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • **inband** - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones.
Enable Privacy	Select this to replace the caller's name and number with "Anonymous". For example, "Anonymous"<Anonymous@172.1.1.253>. Clear this to display caller ID as displayed in this screen's **CallerID Viewer** field.
Proxy Require	Enter this (0~127 alphanumeric characters) to inform the SIP server that this device is behind a firewall or NAT device. Fill this field in only if you were given information by your SIP service provider.
Channel-limit	Specify the maximum number of SIP calls (1~128) allowed to be made through this trunk connection at one time.
Session Timer	
Enable Session Timer	Select this activate the ISG50's session timer. If you encounter connectivity issues with your network or Internet, then it is suggested that you use the session timer.
Minimum SE	Enter the minimum session expiry time in seconds. The allowable range is 90~1800 seconds. When an incoming call requests a session expiry time that is lower than this, the ISG50 uses this value instead.
Session Expires	Enter the session expiry time in seconds for all phone connections on this trunk The allowable range is 90~86400 seconds. This value cannot be lower than the **Minimum SE**. This allows the ISG50 to automatically disconnect any phone calls on this trunk after a certain period of inactivity.

Table 169 Trusted Peer Trunk Add/Edit (continued)

LABEL	DESCRIPTION
CallerID Setting	Configure this section to change the format of identification you want to send when you make VoIP phone calls. The default format is **"From: "Extension"<Extension@Server IP>"**.
CallerID Viewer	This field displays the caller ID format shown to the callees depending on the setting you configure in the **CallerID Name & Number** and **The Extension Prefix** fields.
Representative Number	Specify the representative number shown as source caller ID to the callees when you make external calls through this trunk connection. The default is "**zyxel**".
CallerID Name & Number	Select the caller ID display format you want to use when you make calls. A caller ID consists of a call ID name (**A**), a caller ID number (**B**) and a SIP server IP address (**C**). The caller ID has the following format: "**A**"<**B@C**>. The choices are: (In the following examples, we assume a company representative number is 12345678, their SIP server IP is 10.1.1.1, a caller extension number is 1111 and DDI/DID number 12345555 can map to the extension 1111.) • **Extension + Extension**: Displays the caller's extension number in **A** and **B**. For example, "1111"<1111@10.1.1.1>. • **Extension + Representative Num.**: Displays the caller's extension number in **A** and the SIP trunk's representative number in **B**. For example, "1111"<12345678@10.1.1.1>. • **Representative Num. + Representative Num.**: Displays the SIP trunk's representative number in **A** and **B**. For example, "12345678"<12345678@10.1.1.1>. Select this format if you don't want callees to know the caller's extension number. • **Extension + Representative Num (DDI/DID mapped)**: Displays the caller's extension number in **A** and the SIP trunk's DDI/DID mapped representative number in **B**. For example, "1111"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **B**. • **Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)**: Displays the SIP trunk's DDI/DID mapped representative number in both **A** and **B**. For example, "12345555"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **A** and **B**.
The Extension Prefix	Specify whether to add a prefix number in the callerID name when you make calls through this trunk connection. The availability of this setting varies depending on the format of **CallerID Name & Number** you selected. This field can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and pluses (+)

Table 169 Trusted Peer Trunk Add/Edit (continued)

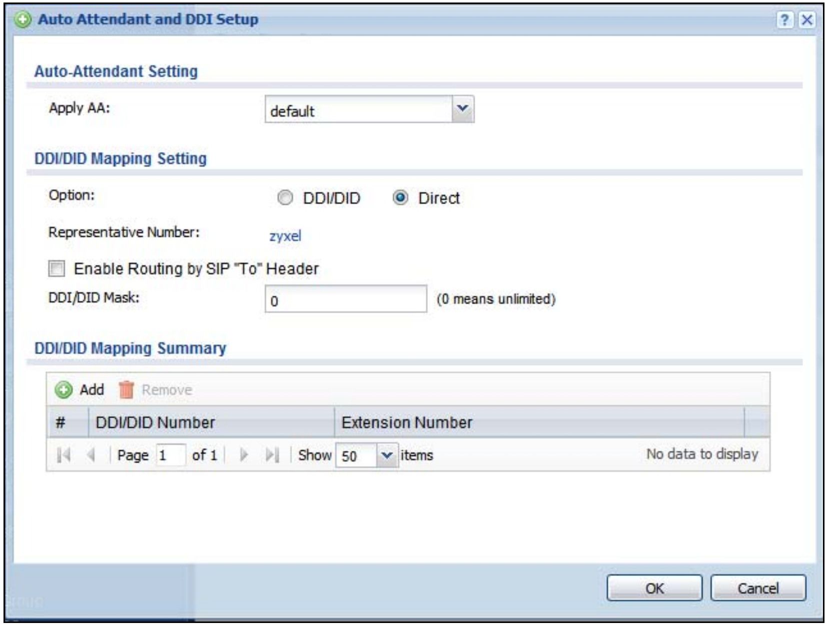
LABEL	DESCRIPTION
Codec Setting	Select the type of voice coder/decoder (codec) that you want this extension to use when communicating with the ISG50. The following codecs (shown in highest quality to lowest quality order) are supported by the ISG50: • **G.711 alaw** (typically used in Europe) • **G.711 ulaw** (typically used in North America and Japan) • **G.729** • **G.722** • **G.723.1** • **G.726** See Voice Codecs on page 475 for more information. When two SIP devices start a SIP session, they must agree on a codec. If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The ISG50 allows the following video codecs to pass through: • **H.261** • **H.263** • **H.264** • **MP4** See Video Codecs on page 475 for more information on video codecs.
Codec Pool	This column indicates the codec types not used for these extensions. You can add a codec type to be used for these extensions by highlighting it and clicking the **Right** button.
Codec List	This column indicates the codec types used by these extensions. You can organize the priority of the codecs by highlighting it and clicking the **Up** or **Down** buttons to move the codec higher or lower in priority. The SIP extensions attempt to use the higher priority codecs first and try the lower priority codecs next. You can remove a codec type from being used from these extension by highlighting it and clicking the **Left** button.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

30.2.5 Trusted Peer Auto Attendant and DDI Setup

Use this screen to select which auto-attendant should be used with this outbound line group. See Chapter 31 on page 503 for information on configuring auto-attendant. You can also configure your

DID (Direct Inward Dialing) settings. In the the **Outbound Trunk Group** configuration screen, select a trusted peer trunk and click the **Auto-Attendant** icon to view the screen as shown.

Figure 316 Trusted Peer Auto Attendant and DDI Setup



Apply AA: default

Option: ○ DDI/DID ● Direct

Representative Number: zyxel

☐ Enable Routing by SIP "To" Header

DDI/DID Mask: 0 (0 means unlimited)

#	DDI/DID Number	Extension Number

No data to display

Each field is described in the following table.

Table 170 Trusted Peer Auto Attendant and DDI Setup

LABEL	DESCRIPTION
Auto-Attendant Setting	
Apply AA	Select an Auto-Attendant or ACD skill profile used for the calls incoming through this outbound line trunk. Select **default** to forward all incoming calls on this outbound line group according to each extension's settings. Select **ACD** if you want to forward all incoming calls on this outbound line group to the group of agents associated with a specific skill name. Select **FAX** if you want to forward all incoming calls on this outbound line group to a fax machine located at a specific extension. Select **Extension** if you want to directly forward all incoming calls through this outbound line group to an extension.
Skill	This field displays if you select **ACD** in the **Apply AA** field. Select the skill name of the agents to associate with this outbound line trunk.
Extension Number for Fax	This field is only available if you select **FAX** in the **Apply AA** field. Type the extension of the Fax machine you want to forward calls to.
Extension Number	This field is only available if you select **Extension** in the **Apply AA** field. Type an extension you want to forward calls to.
DDI/DID Mapping Setting	
Option	Select **DDI/DID** to map a dialed number through this outbound line group to an extension or direct it to the auto attendant for incoming calls. Select **Direct** to forward all incoming calls through this outbound line group directly to their called numbers.

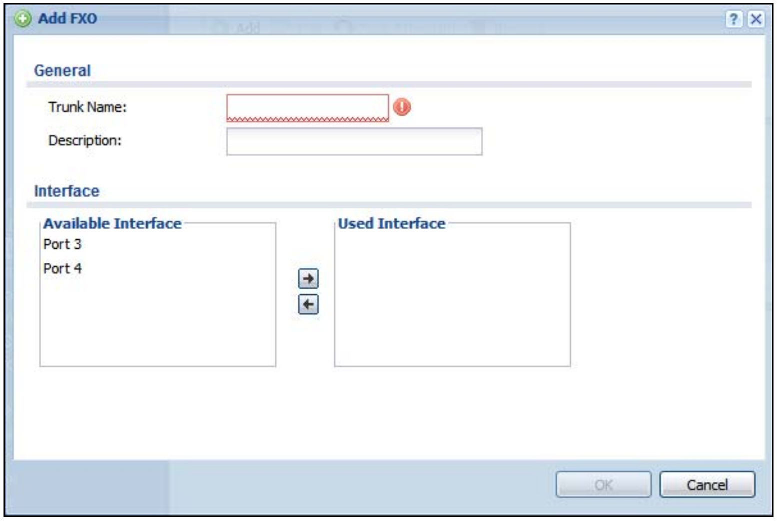
Table 170 Trusted Peer Auto Attendant and DDI Setup

LABEL	DESCRIPTION
Representative Number	This field displays the representative number configured for the trunk.
Enable Routing by SIP "To" Header	Select this if this auto-attendant interacts with a SIP server that uses the SIP To header to do the DDI/DID mapping. If this trunk outbound line group has DDI/DID mode enabled, using this deletes all of the this trunk outbound line group's DDI/DID mapping settings and sets the **DDI/DID Mask** to 0. Clear this to use the SIP request URI to do the DDI/DID mapping.
DDI/DID Mask	Enter a number (0~10) to decide the number of digits you want to enter for the next DDI/DID number(s). 0 means you can enter any number of digits for the next DDI/DID number(s).
DDI/DID Mapping Summary	Use this section to manage the DDI/DID numbers which allow outsiders to call and reach extensions directly.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. See Section 30.2.3 on page 488 for a description of adding a DDI/DID mapping.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
DDI/DID Number	This field shows the DDI/DID number outsiders can call to reach the entry's extension directly.
Extension Number	This field shows the extension that outsiders can reach directly by calling the entry's DDI/DID number.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.6 Add/Edit FXO Trunk

The screens for editing or adding FXO trunks on the ISG50 contain the same fields. Only the screen used to add FXO trunks is shown below. Click the **Add** (or **Edit**) icon in the **FXO Trunk** section of the **Outbound Trunk Group** configuration screen to view the screen as shown.

Figure 317 Add/Edit FXO Trunk



Each field is described in the following table.

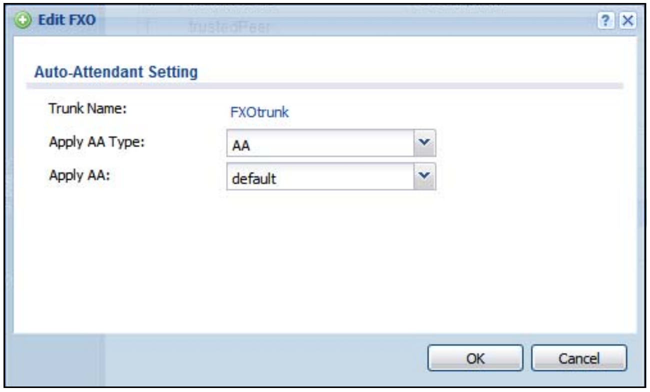
Table 171 Add/Edit FXO Trunk

LABEL	DESCRIPTION
Trunk Name	Type the name of this FXO interface group. This field can be 1-30 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). The first character must be a letter.
Description	Type the description for this FXO interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Available Interface	This column displays the FXO ports available on the ISG50. Highlight one of the FXO ports and click the **Right** icon if you want to add it to this outbound line group.
Used Interface	This column displays the FXO ports currently configured for this outbound line group. Highlight one of the FXO ports and click the **Left** icon if you want to remove it from the outbound line group. If you configure more than one interfaces in this outbound line group, the ISG50 check and pick one of them available for an outgoing call.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.7 FXO or BRI Auto Attendant

Use this screen to select which auto-attendant should be used with this outbound line group. See Chapter 31 on page 503 for information on configuring auto-attendant. In the **Outbound Trunk Group** configuration screen, select an FXO or BRI trunk and click the **Auto-Attendant** icon to view the screen as shown.

Figure 318 AA for FXO or BRI Trunk



Trunk Name: FXOtrunk
Apply AA Type: AA
Apply AA: default

Each field is described in the following table.

Table 172 AA for FXO or BRI Trunk

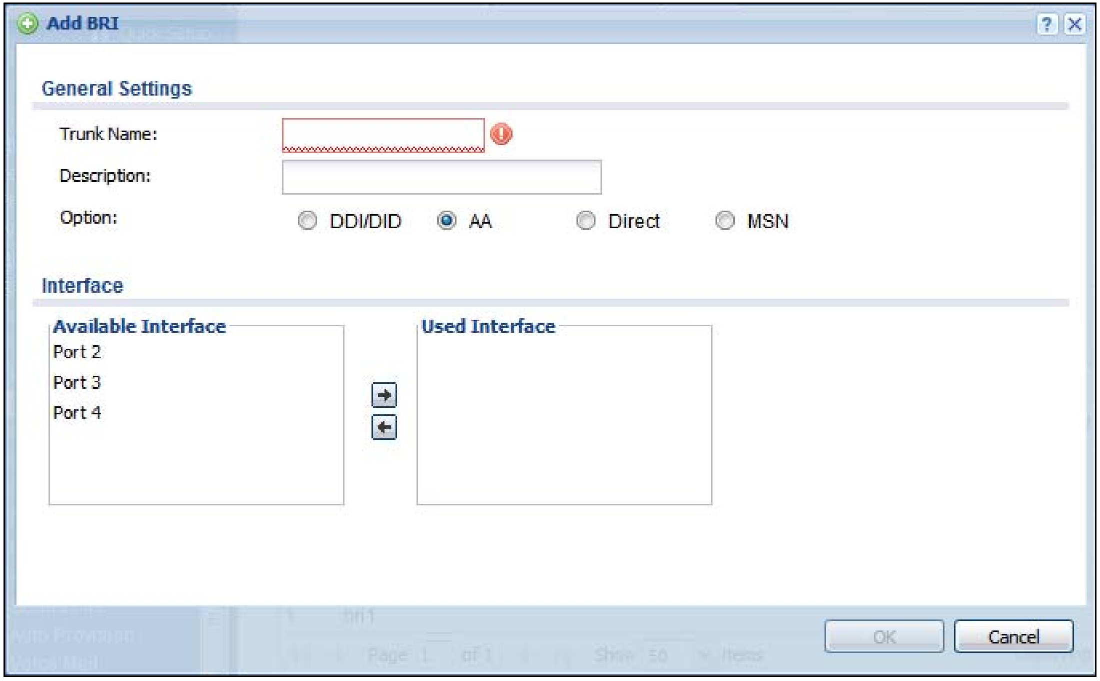
LABEL	DESCRIPTION
Trunk Name	This field displays the name of the outbound line trunk.
Apply AA Type	Select the auto attendant you want to use when calls come in on this outbound line group. Select **AA** (Auto-Attendant) to forward all calls coming in through this outbound line group to an Auto-Attendant system first. Select **Extension** to directly forward all calls coming in through this outbound line group to an extension. At least one extension must already exist in the ISG50 for this option to display. Select **FAX** to forward all calls coming in through this outbound line group to a fax machine located at a specific extension. At least one extension must already exist in the ISG50 for this option to display. Select **ACD Skill** to forward all calls coming in through this outbound line group to the group of agents associated with this skill name. An extension must already exist to get this option. At least one ACS skill must already exist in the ISG50 for this option to display.
Apply AA	Select an Auto-Attendant or ACD skill profile used for the calls incoming through this outbound line trunk.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.8 Add/Edit BRI Trunk

Use this screen to configure a BRI Trunk. The fields vary depending on how the ISG50 handles incoming and outgoing calls you configured in the **Option** field. Click the **Add** icon in the **BRI**

Settings section of the **Outbound Trunk Group** configuration screen to view the screen as shown.

Figure 319 BRI Trunk - Add/Edit: AA



Add BRI
General Settings
Interface
Available Interface
Used Interface
OK
Cancel

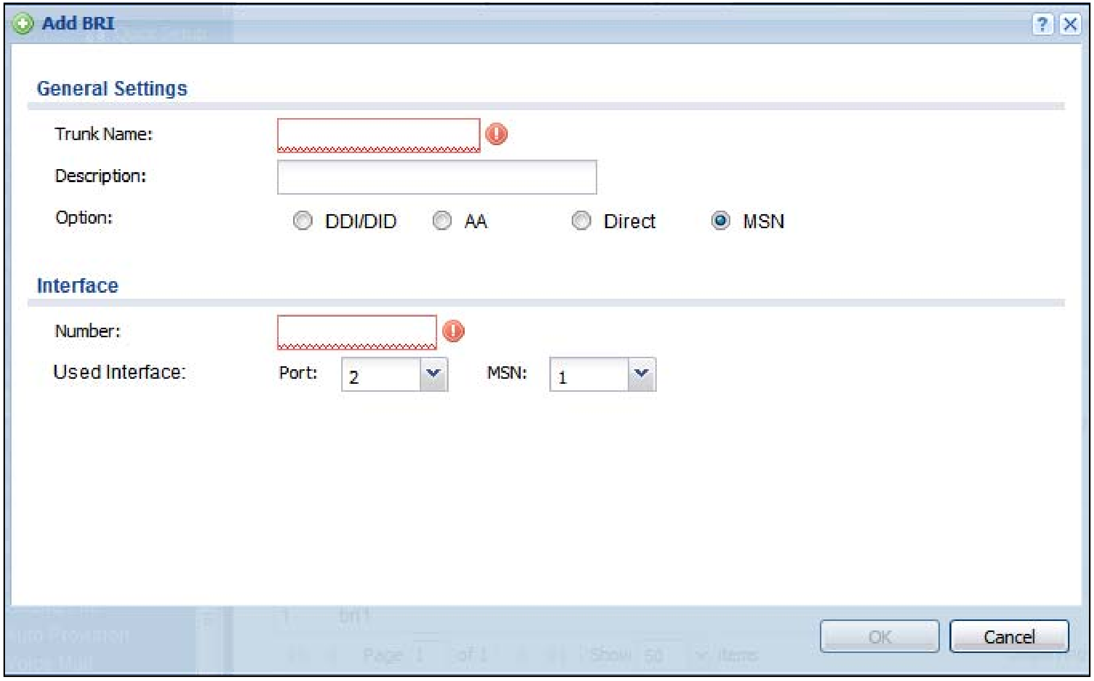
Trunk Name:

Description:

Option: ○ DDI/DID ● AA ○ Direct ○ MSN

Available Interface: Port 2, Port 3, Port 4

Figure 320 BRI Trunk - Add/Edit: MSN



Add BRI
General Settings
Interface
OK
Cancel

Trunk Name:

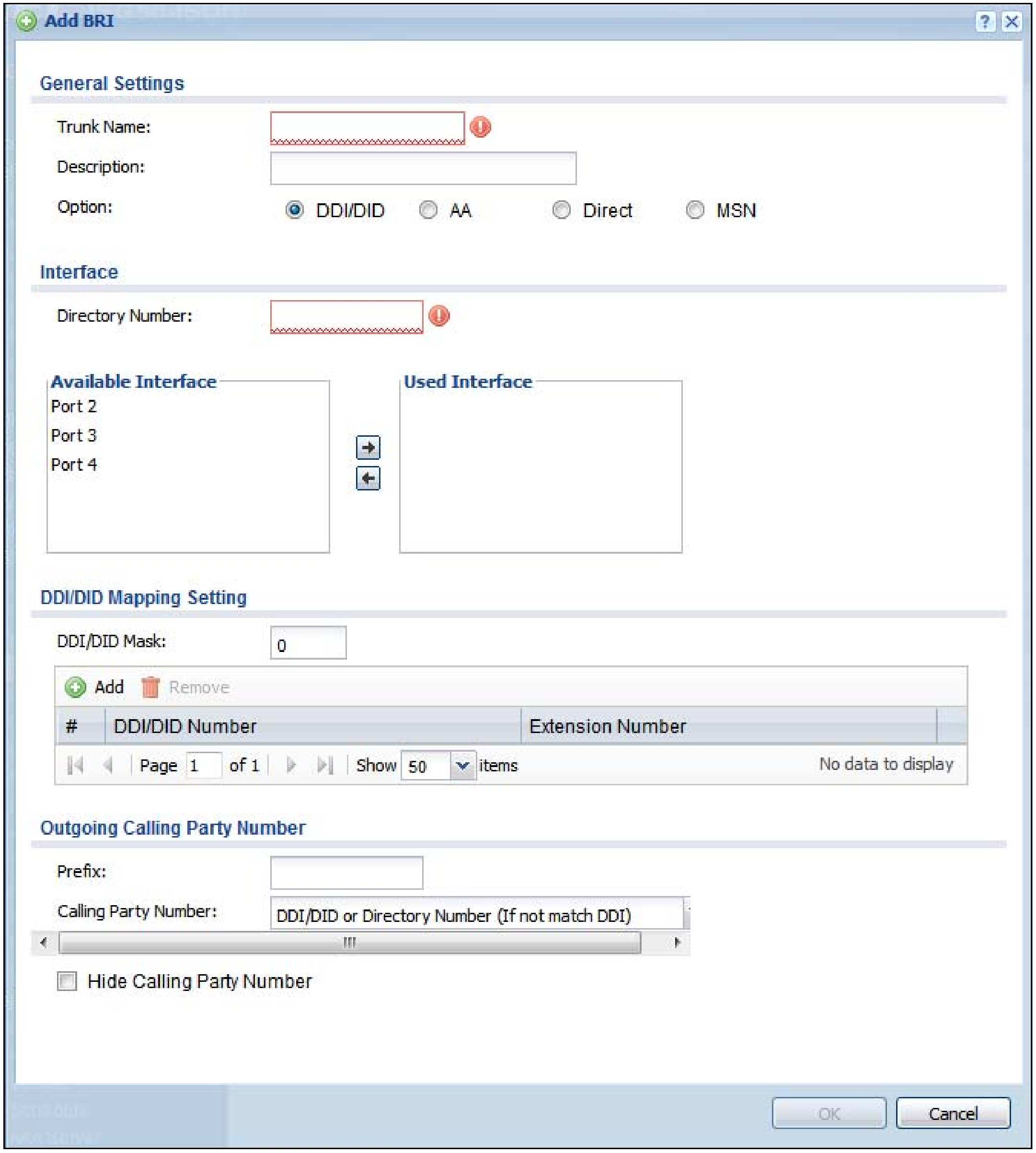
Description:

Option: ○ DDI/DID ○ AA ○ Direct ● MSN

Number:

Used Interface: Port: 2 MSN: 1

Figure 321 BRI Trunk - Add/Edit: DDI/DID


Add BRI
General Settings
Interface
Available Interface
Used Interface
DDI/DID Mapping Setting
Add
Remove
Outgoing Calling Party Number
OK
Cancel

Trunk Name:

Description:

Option: ● DDI/DID ○ AA ○ Direct ○ MSN

Directory Number:

Available Interface: Port 2, Port 3, Port 4

DDI/DID Mask: 0

#	DDI/DID Number	Extension Number

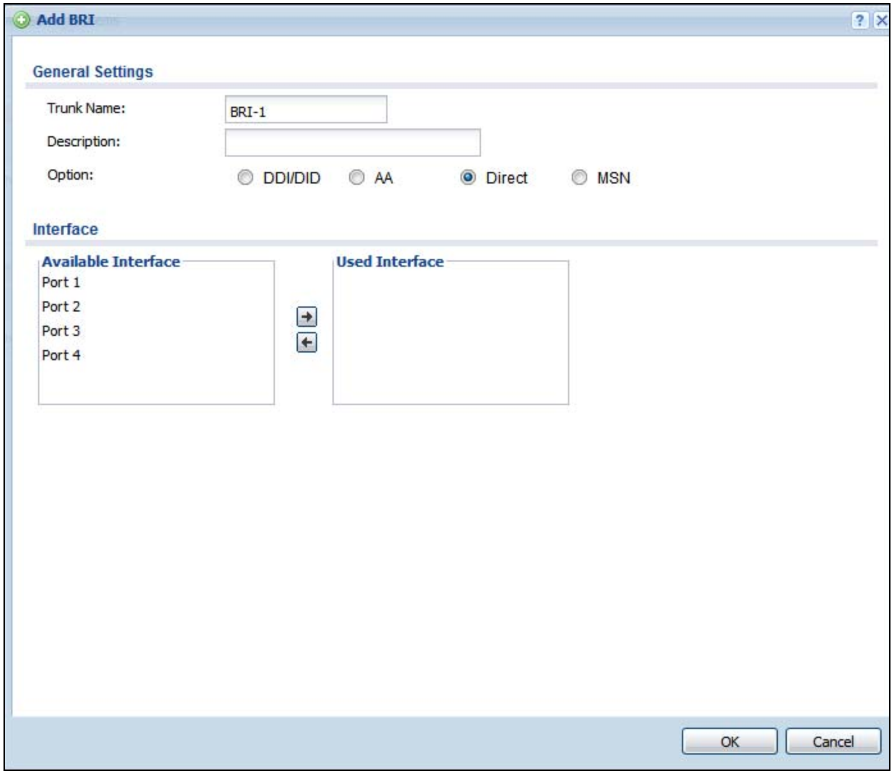
Page 1 of 1 Show 50 items No data to display

Prefix:

Calling Party Number: DDI/DID or Directory Number (If not match DDI)

☐ Hide Calling Party Number

Figure 322 BRI Trunk - Add/Edit: Direct



Trunk Name: BRI-1

Description:

Option: ○ DDI/DID ○ AA ● Direct ○ MSN

Available Interface: Port 1, Port 2, Port 3, Port 4

Used Interface:

Each field is described in the following table.

Table 173 BRI Trunk Add/Edit

LABEL	DESCRIPTION
General Settings	
Trunk Name	Type the name of this BRI interface. This field can be 1-30 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). The first character must be a letter.
Description	Type the description for this BRI interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Option	Specify the service type for this BRI trunk. Select **DDI/DID** (Direct Dialing In) when you want people to use a “direct number” to dial an outgoing call. You can also specify a prefix number in the caller number that might be required by your telephone company for outgoing calls using **DDI/DID**. See DDI (Direct Dial In) on page 479 for more information. Select **AA** (Auto-Attendant) to switch all calls coming through this interface to the Auto-Attendant system first. See Section 31.1 on page 503 for more information. Select **Direct** to forward all calls coming through this interface from trusted callers to extensions. See Calling Directly to an Extension on page 480 for more information. Select **MSN** (Multiple Subscribe Number) to switch all the calls to MSNs coming through this interface to the Auto-Attendant system first. See Using Multiple ISDN Numbers on page 478 for more information.
Directory Number	Enter your ISDN number registered to your telephone company. This number is used for the caller number when you make an outgoing call through the trunk from the extension which cannot be found in the DDI mapping table. This field can be 3-20 digits in length.

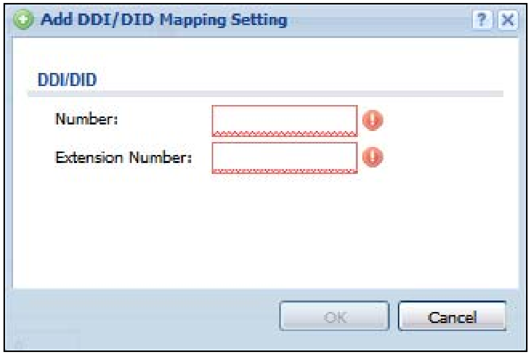
Table 173 BRI Trunk Add/Edit (continued)

LABEL	DESCRIPTION
Available Interface	For **DDI/DID**, **AA**, and **Direct**, this list displays the available slots and ports on the ISG50. Click one slot and port and then click the **Right** icon if you want to add it to this outbound group.
Used Interface	For **DDI/DID**, **AA**, and **Direct**, this list displays the ports currently configured for this outbound line group. Click one port and click the **Left** icon if you want to remove it from the outbound group. If you configure more than one interfaces in this outbound line group, the ISG50 check and pick one of them available for an outgoing call.
Number	This field displays for **MSN**. There the MSN number the interface is to use.
Used Interface	This field displays for **MSN**. Select the BRI port and the MSN number the interface is to use.
DDI/DID Mapping Setting	Use this section to configure your DDI mapping table.
DDI/DID Mask	Enter a number (0~20) to identify the extension mapping digits from right to left, so a DDI mask of 2 applied to the incoming ISDN number 555-123456 would identify the numbers 56.
Add	Click this to add a new entry to the local net list.
Remove	Click this to delete the selected item(s) in this list.
#	This field is a sequential value, and it is not associated with a specific entry.
DDI/DID Number	This is the DDI number.
Extension Number	This is the DDI number’s associated extension number.
Outgoing Calling Party Number	
Prefix	Enter a number to add in the beginning of the outgoing caller’s numbers using this trunk line. This field can be 0-20 digits in length.
Calling Party Number	Use this section to set your outgoing calling party numbers. These are what the callee sees when the ISG50 sends a call out through this BRI trunk. **DDI/DID or Directory Number (If not match DDI)** - Select this to have calls going out through this BRI trunk use the DDI/DID if the outgoing call matches it or the number defined in the **Directory Number** field if the outgoing call does not match the DDI/DID. **Directory Number** - Select this to have calls going out through this BRI trunk use the number defined in the **Directory Number** field. **DDI/DID or User Define Number (If not match DDI)** - Select this to have calls going out through this BRI trunk use the DDI/DID if the outgoing call matches it or another number that you specify if the outgoing call does not match the DDI/DID. Enter the number in the field. This field can be 3-20 digits in length. **User Define** - Select this to have calls going out through this BRI trunk use a number that you specify. Enter the number in the field. This field can be 3-20 digits in length. **Extension** - Select this to have calls going out through this BRI trunk use the caller’s extension number.
Hide Calling Party Number	Select this to not have your calling party number display on the callee’s caller ID. This option only applies to calls going out through this BRI trunk that do not match the DDI/DID.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.9 Add BRI Trunk DDI/DID Mapping

Use this screen to add or edit DDI/DID mapping table entries. Click the **Add** icon in the **DDI/DID Mapping Setting** section of the **BRI Trunk - Add** configuration screen to view the screen as shown.

Figure 323 Add BRI Trunk DDI/DID Mapping



Each field is described in the following table.

Table 174 Add BRI Trunk DDI/DID Mapping

LABEL	DESCRIPTION
Number	Enter the DDI number. This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.
Extension Number	Enter the DDI number's associated extension number. This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

30.2.10 Auto-Attendant for Incoming BRI Calls

Use this screen to select which auto-attendant should be used with this outbound line group. The fields in this screen are the same as the fields in the FXO trunk auto-attendant screen. Refer to Section 30.2.7 on page 496 for detailed field descriptions.

31

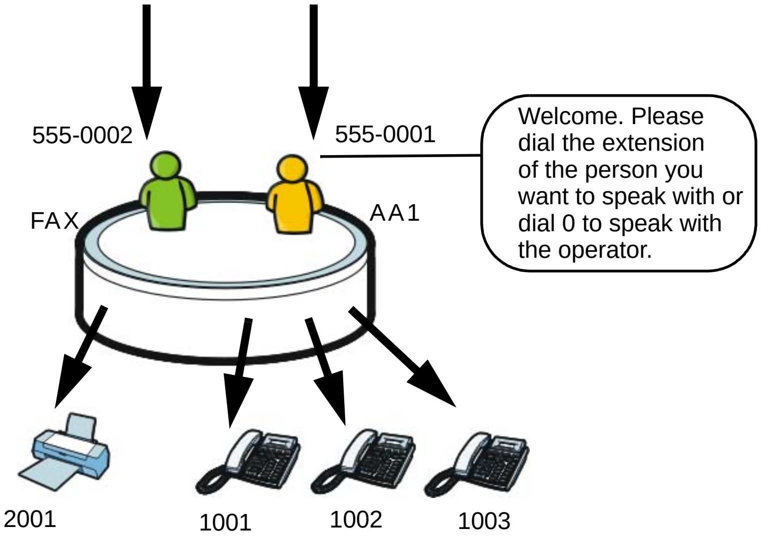
Auto-attendant

31.1 Overview

This chapter shows you how to configure auto-attendant on the ISG50.

An auto-attendant is software which acts as an automatic switchboard operator. Auto-attendants help route incoming calls to their proper extension. An auto-attendant is assigned to each outbound line group and it services incoming calls on those lines. If your organization has two outbound line groups, each with a specific telephone number for incoming calls, then you can assign a different auto-attendant for each incoming line. Assign one auto-attendant for general calls to your organization (for example, **AA1**) and one auto-attendant (for example **FAX**) for direct routing to a fax machine.

Figure 324 Auto-Attendant Overview


555-0002
555-0001
Welcome. Please dial the extension of the person you want to speak with or dial 0 to speak with the operator.
FAX
AA1
2001
1001
1002
1003

31.1.1 What You Can Do in this Chapter

- Use the **Default** screen to configure the default auto-attendant used by all trunks when a custom auto-attendant does not exist or apply. See Section 31.2 on page 505.
- Use the **Customized** screen to view, add, edit or delete auto-attendants from the ISG50. See Section 31.3 on page 507.

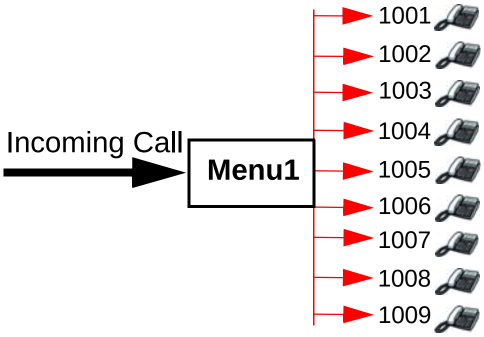
31.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Default Auto-Attendant Structure

The ISG50 comes with a default auto-attendant. The default auto-attendant simply prompts callers to enter the extension they wish to reach. There is only one time when a caller has to make a decision. The following figure shows the default auto-attendant structure.

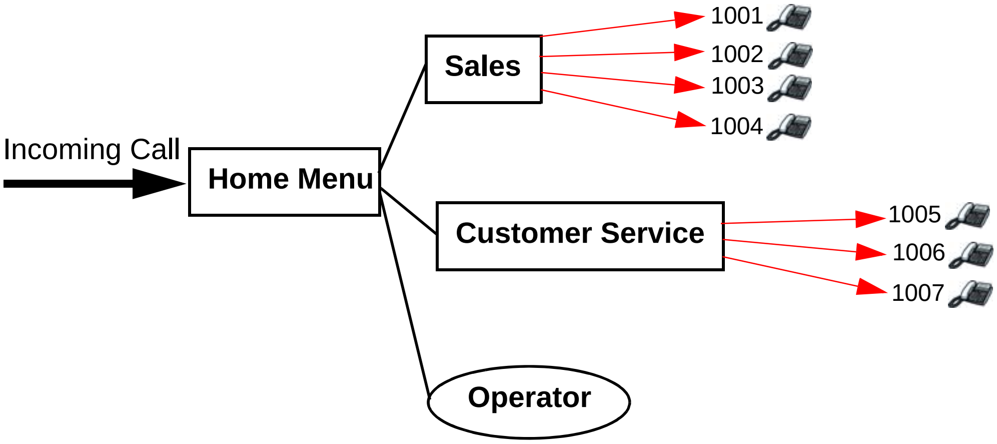
Figure 325 Auto-Attendant Default Structure Example



Custom Auto-Attendant Structure

You can configure a more complex auto-attendant structure to fit your organization's needs. An auto-attendant can contain several more complex menus that can guide an incoming call to a specific extension or a group of extensions. In the following example, an incoming caller is prompted to specify whether they want to talk to a sales representative, customer service representative or the operator. Once the caller reaches the **Sales** menu, the auto-attendant can prompt them to specify which product they are interested in. The caller then dials a number to reach the appropriate sales representative.

Figure 326 Auto-Attendant Custom Structure Example



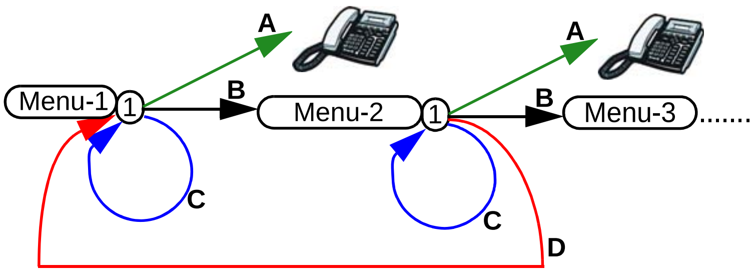
Configuring Menus

Configuring an auto-attendant requires you to set up menus. In Figure 326 on page 504 there are three menus. The **Home Menu** and two sub menus: **Sales** and **Customer Service**. Each menu should have an accompanying audio file which informs the callers of their options. In each menu you can allow or disallow the dialing of extensions. You can also assign the following options to each menu based on the action performed by the caller. Each option is followed by example content for the accompanying audio file.

- Direct a call to an extension. “Dial 1 to reach the operator.”
- Direct a caller to the next menu. “Dial 2 to reach the sales department.”
- Allow the caller to listen to the current menu again. “Dial 3 to listen to this menu again.”
- Allow the caller to go back to the previous menu. “Dial 4 to go back to the previous menu.” (Not available for the first menu.)

The caller dials the number specified in the prompt to navigate through the auto-attendant’s menus. When configuring auto-attendant, you must choose a number that the caller should dial and an associated function for that option. The following example shows the options you can assign when the caller dials 1 as he or she moves through your customized auto-attendant.

Figure 327 Auto-Attendant Menus



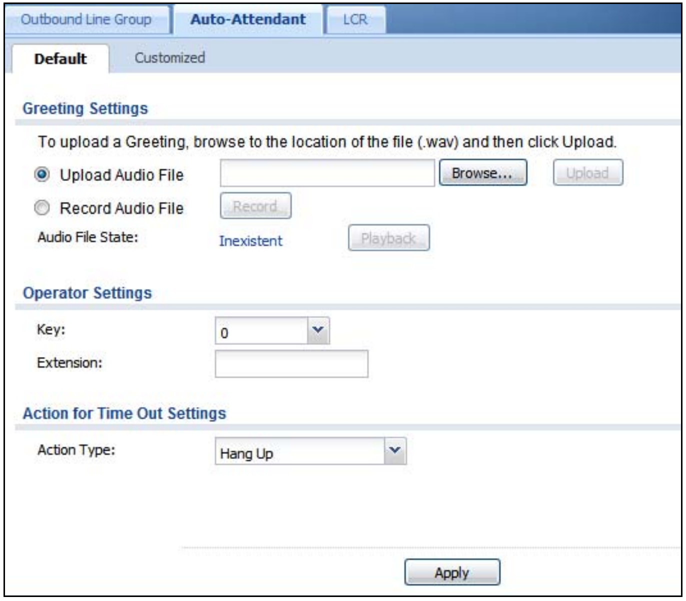
When a caller dials **1** in **Menu-1**, you can direct them to an extension (**A**), move them to the next menu (**B**) or allow them to hear the menu again (**C**). The same options are available in **Menu-2** with the addition of going back to **Menu-1** (**D**).

31.2 The Default Auto-Attendant Screen

Use this screen to configure the default auto-attendant used by all trunks when a custom auto-attendant does not exist or apply. These settings are used if a custom auto-attendant is not assigned.

Click **Configuration > PBX > Outbound Line Management > Auto-Attendant** to view the screen as shown next.

Figure 328 Auto-Attendant > Default


Outbound Line Group
Auto-Attendant
LCR
Default
Customized
Greeting Settings
Browse...
Upload
Record
Playback
Operator Settings
Action for Time Out Settings
Apply

To upload a Greeting, browse to the location of the file (.wav) and then click Upload.

● Upload Audio File

○ Record Audio File

Audio File State: Inexistent

Key: 0

Extension:

Action Type: Hang Up

Each field is described in the following table.

Table 175 Auto-Attendant > Default

LABEL	DESCRIPTION
Greeting	
Upload Audio File	Click **Browse** to locate an audio file to be used as the auto-attendant greeting message, and **Upload** to copy it to the ISG50. The audio file you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The total play time of all the AA audio files combined must be less than 30 minutes.
Record Audio File	Click this to record an audio file through the extension set as the recording peer.
Audio File State	This indicates whether an audio file has been uploaded to the ISG50 or not. You can also **Playback** the audio file to hear how it sounds.
Operator Settings	
Key	Select either **0** or **9** to be the default operator key. When a caller presses the operator key, his calls is routed to the associated **Extension**.
Extension	Enter an extension number to associate with the operator **Key**. When that key is pressed, the call is routed to this extension.

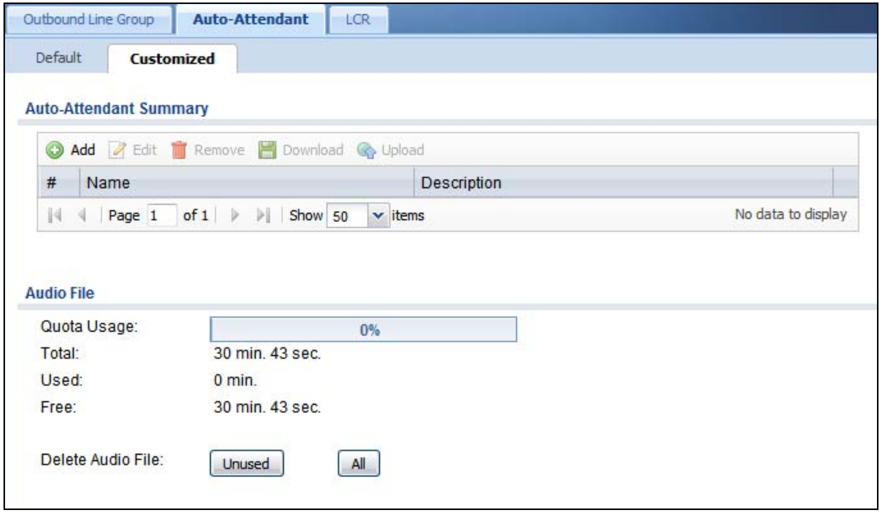
Table 175 Auto-Attendant > Default (continued)

LABEL	DESCRIPTION
Action Type	Select how the auto-attendant should proceed if no key is pressed for 5 seconds or the caller inputs an incorrect key code three times in a row. • **Hang Up** disconnects the call. • **Extension** routes the call to the specified extension. • **ACD** engages the ACD system. See Chapter 38 on page 553 for details on this feature. • **Page Group** forwards the call to the page group you specify. See Chapter 37 on page 549 for details on this feature. • **Hunt Group** forwards the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Auto Attendant** forwards the call to the auto attendant you specify. See Chapter 31 on page 503 for details on this feature. • **User Defined Number** forwards the call to the extension or other phone number you specify. Enter a number 3-20 digits in length.
Apply	Click this to save your changes.

31.3 The Customized Auto-Attendant Screen

Use this screen to view, add, edit or delete auto-attendants from the ISG50. To access this screen, click **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized**.

Figure 329 Auto-Attendant > Customized


Outbound Line Group
Auto-Attendant
LCR
Default
Customized
Auto-Attendant Summary
Add
Edit
Remove
Download
Upload
#
Name
Description
Page 1 of 1
Show 50 items
No data to display
Audio File

Quota Usage: 0%
Total: 30 min. 43 sec.
Used: 0 min.
Free: 30 min. 43 sec.

Delete Audio File:
Unused
All

Each field is described in the following table.

Table 176 Auto-Attendant > Customized

LABEL	DESCRIPTION
Auto-Attendant Summary	Use this section to manage your custom auto attendants.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.

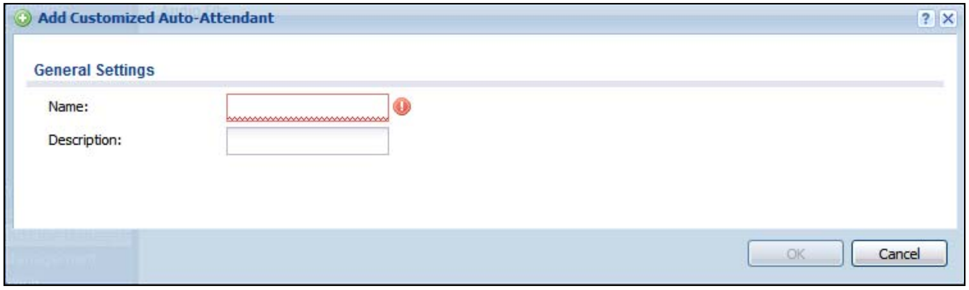
Table 176 Auto-Attendant > Customized (continued)

LABEL	DESCRIPTION
Download	Select an entry and click **Download** to save the selected auto-attendant's audio files to your computer.
Upload	Select an entry and click **Upload** to upload a backup audio file for it.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This field displays the name assigned to an auto-attendant.
Description	This field displays the description for an auto-attendant.
Audio File	Use this section to manage your auto attendant audio files.
Quota Usage	This bar displays what percentage of the ISG50's audio file storage space is currently in use. When the storage space is almost full, you should consider deleting unused audio files before adding more.
Total	This is the ISG50's total available audio recording time.
Used	This is how much of the ISG50's audio recording time is already used.
Free	This is the ISG50's remaining available audio recording time.
Delete Audio File	Click **Unused** to delete the audio recordings that not none of the ISG50's features are set to use or **All** to delete all of the audio recordings.

31.3.1 The Add/Edit Auto-Attendant Screen

Use this screen to add or edit an auto-attendant. To access this screen, click the **Add** or **Edit** icon in the **Configuration** > **PBX** > **Outbound Line Management** > **Auto-Attendant > Customized** screen to view the screen as shown.

Figure 330 Auto-Attendant > Add/Edit



Each field is described in the following table.

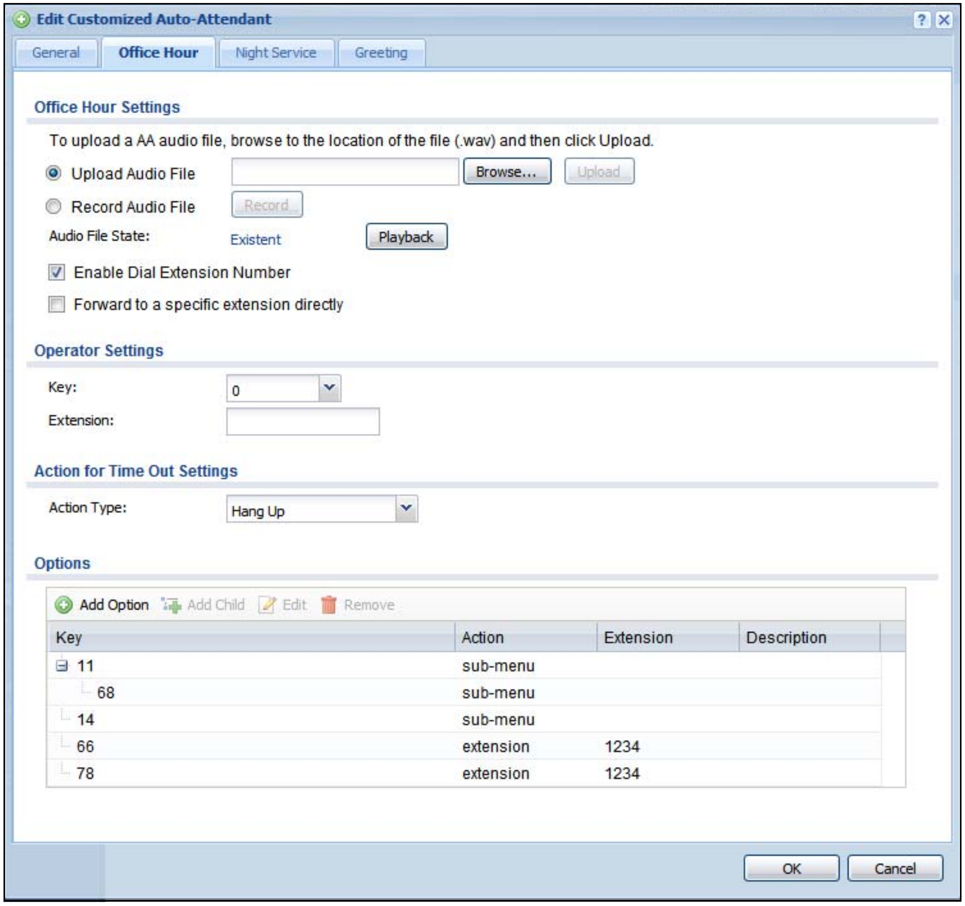
Table 177 Auto-Attendant > Add/Edit

LABEL	DESCRIPTION
Name	Type a name for this auto-attendant. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type a description for this auto-attendant. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9) and spaces. 0 means this field can be left blank.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

31.3.2 Auto Attendant Settings: Office Hours

Use this screen to edit auto-attendant office hour settings. To access this screen, click the **Add** or **Edit** icon in the **Configuration** > **PBX** > **Outbound Line Management** > **Auto-Attendant > Customized** screen and then click the **Office Hour** tab.

Figure 331 Office Hours Setting


Edit Customized Auto-Attendant
General
Office Hour
Night Service
Greeting
Office Hour Settings
Browse...
Upload
Record
Playback
Operator Settings
Action for Time Out Settings
Options
Add Option
Add Child
Edit
Remove
OK
Cancel

To upload a AA audio file, browse to the location of the file (.wav) and then click Upload.

● Upload Audio File

○ Record Audio File

Audio File State: Existent

☑ Enable Dial Extension Number

☐ Forward to a specific extension directly

Key: 0

Extension:

Action Type: Hang Up

Key	Action	Extension	Description
⊟ 11	sub-menu		
68	sub-menu		
14	sub-menu		
66	extension	1234	
78	extension	1234	

Each field is described in the following table.

Table 178 Office Hours Setting

LABEL	DESCRIPTION
Office Hour Settings	
Upload Audio File	Click **Browse** to locate an audio file to be used as the auto-attendant greeting message, and **Upload** to copy it to IP-PBX. The audio file you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The total play time of all the AA audio files combined must be less than 30 minutes.
Record Audio File	Click this to record an audio file through the extension set as the recording peer.
Audio File State	This indicates whether an audio file has been uploaded to the ISG50 or not. You can also **Playback** the audio file to hear how it sounds.
Enable Dial Extension Number	Select this to allow incoming calls to dial extensions that are not associated with specific key codes on the **Options** list below. Clear it to limit all input to the key codes listed on the **Options** table below.

Table 178 Office Hours Setting (continued)

LABEL	DESCRIPTION
Forward to a specific extension directly	Select this option to forward all calls that come into this auto-attendant to the specified extension, ACD, page group, hunt group, or user defined number.
Play audio file before forward to a specific extension	Select this option to play the uploaded audio file before forwarding the call to the specified extension, ACD, page group, hunt group, or user defined number.
Operator Settings	
Key	Select either **0** or **9** to be the default operator key. When a caller presses the operator key, his calls is routed to the associated **Extension**.
Extension	Enter an extension number to associate with the operator **Key**. When that key is pressed, the call is routed to this extension.
Action for Time Out	Select how the auto-attendant should proceed if no key is pressed for 5 seconds or the caller inputs an incorrect key code three times in a row. • **Hang Up** disconnects the call. • **Extension** routes the call to the specified extension. • **ACD** engages the ACD system. See Chapter 38 on page 553 for details on this feature. • **Page Group** forwards the call to the page group you specify. See Chapter 37 on page 549 for details on this feature. • **Hunt Group** forwards the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Auto Attendant** forwards the call to the auto attendant you specify. See Chapter 31 on page 503 for details on this feature. • **User Defined Number** forwards the call to the extension or other phone number you specify. Enter a number 3-20 digits in length.
Options	This section displays the actions configured for this auto-attendant menu.
Add Option	Click this to create a new option entry.
Add Child	Select an option entry that displays **sub-menu** as the **Action** and click this to create a sub-entry. See Section 31.3.4 on page 512 for details.
Edit	Select an entry and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Key	This field displays the digits a caller must dial to perform an action.
Action	This field displays the function of an option.
Extension	This field displays either the extension, hunting group or ACD number that this call is forwarded to or it is blank if the action for this auto-attendant option is set to **Forward to a sub menu**. Click **Next Menu** to configure the settings for a sub menu.
Description	This field displays the description for this action.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

Auto-Attendant Audio Files

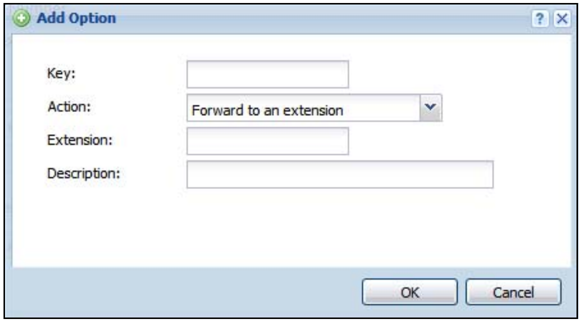
You can record your own custom auto-attendant messages. The audio files you record must meet the following criteria:

- PCM format, 16 kHz, 16-bit, mono mode (*.wav).
- The total play time of all the AA audio files combined must be less than 30 minutes.

31.3.3 The Add/Edit Auto-Attendant Option Screen

Use this screen to configure an option for an auto-attendant menu. To access this screen, click the **Add** or **Edit** icon for an item in the office hour or night service **Options** list.

Figure 332 Add/Edit Option Setting



Action: Forward to an extension

Each field is described in the following table.

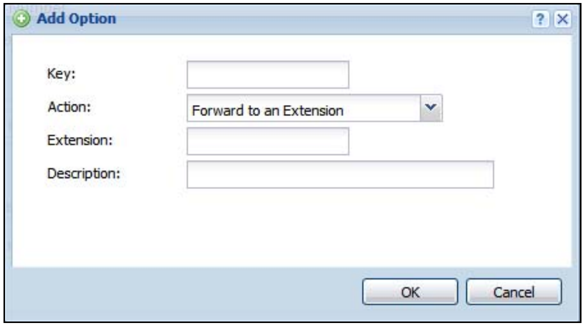
Table 179 Add/Edit Option Setting

LABEL	DESCRIPTION
Key	Type the digit(s) a caller should dial to execute this option. This field can be 1-2 digits in length.
Action	Specify the action for this auto-attendant option. The choices are: • **Forward to an extension** - to forward a call to a specific extension. • **Forward to a skill** - to route the call to an ACD skill. See Chapter 38 on page 553 for details on using this feature. • **Forward to page group** - to forward the call to the page group you specify. See Chapter 37 on page 549 for details on this feature. • **Forward to hunt group** - to forward the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Forward to an Auto-Attendant** - to forward the call to the auto attendant you specify. See Chapter 31 on page 503 for details on this feature. • **Forward to an user defined number** - to forward the call to the extension or other phone number you specify. Enter a number 3-20 digits in length. • **Forward to a sub menu** - to forward a call to child menu that you configure. • **Repeat menu** - to replay the auto-attendant audio file for this menu.
Extension	Specify the extension or a hunting group number you want to forward this call to. This field is only applicable if you select **Forward to an extension** in the **Action** field. This field can be 3-20 digits in length.
Description	Type a description for this auto-attendant option. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9) and spaces. 0 means this field can be left blank.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

31.3.4 The Auto-Attendant Sub Menu Screen

Use this screen to configure an option for an auto-attendant sub menu (child menu). To access this screen, in the auto-attendant **Office Hour** or **Night Service** screen, select an option entry that displays **sub-menu** as the **Action** and click **Add Child**.

Figure 333 Auto-Attendant Sub Menu



Action: Forward to an Extension

Each field is described in the following table.

Table 180 Auto-Attendant Sub Menu

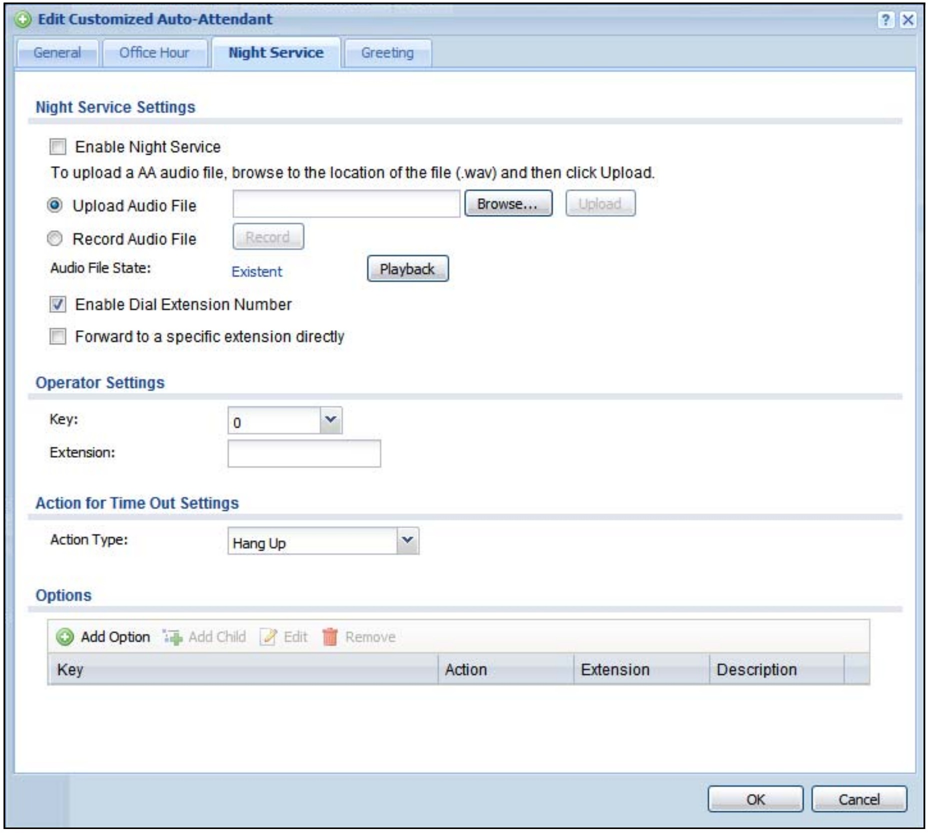
LABEL	DESCRIPTION
Key	Type the digit(s) a caller should dial to execute this option. This field can be 1-2 digits in length.
Action	Specify the action for this auto-attendant option. The next field changes based on the action you specify. The choices are: • **Forward to an extension** - to forward a call to a specific extension. • **Forward to a skill** - to route the call to an ACD skill. See Chapter 38 on page 553 for details on using this feature. • **Forward to page group** - to forward the call to the page group you specify. See Chapter 37 on page 549 for details on this feature. • **Forward to hunt group** - to forward the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Forward to an Auto-Attendant** - to forward the call to the auto attendant you specify. See Chapter 31 on page 503 for details on this feature. • **Forward to a user defined number** - to forward the call to the extension or other phone number you specify. Enter a number 3-20 digits in length. • **Forward to a sub menu** - to forward a call to child menu that you configure. • **Repeat menu** - to replay the auto-attendant audio file for this menu.
Extension	Specify the extension to which to forward the call. This field can be 3-20 digits in length.
ACD	Select the ACD skill to which to forward the call. The ACD skill must already be configured.
Number	Select the page or hunt group to which to forward the call. The ACD skill must already be configured.
Auto-Attendant	Select the auto attendant to which to forward the call. The ACD skill must already be configured.
Extension	Specify the extension or phone number to which to forward the call. This field can be 3-20 digits in length.
Description	Type a description for this auto-attendant option. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9) and spaces. 0 means this field can be left blank.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

31.3.5 Auto Attendant Settings: Night Service

Use this screen to configure **Night Service** settings for this auto-attendant. You only need to configure this screen if you want the auto-attendant to perform different actions outside of regular office hours.

In the **Configuration** > **PBX** > **Outbound Line Management** > **Auto-Attendant > Customized** screen click the **Add** or **Edit** icon for an item in the auto-attendant list and select the **Night Service** tab to view a screen as shown next.

Figure 334 Night Service Setting



Night Service Settings

☐ Enable Night Service

To upload a AA audio file, browse to the location of the file (.wav) and then click Upload.

● Upload Audio File

○ Record Audio File

Audio File State: Existent

☑ Enable Dial Extension Number

☐ Forward to a specific extension directly

Operator Settings

Key: 0

Extension:

Action for Time Out Settings

Action Type: Hang Up

Options

Key	Action	Extension	Description

Each field is described in the following table.

Table 181 Night Service Setting

LABEL	DESCRIPTION
Enable Night Service	Select this to activate the night service settings for this auto-attendant or clear it to turn them off.
Upload Audio File	Click **Browse** to locate an audio file to be used as the auto-attendant greeting message, and **Upload** to copy it to IP-PBX. The audio file you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The total play time of all the AA audio files combined must be less than 30 minutes.
Record Audio File	Click this to record an audio file through the extension set as the recording peer.
Audio File State	This indicates whether an audio file has been uploaded to the ISG50 or not. You can also **Playback** the audio file to hear how it sounds.

Table 181 Night Service Setting (continued)

LABEL	DESCRIPTION
Enable Dial Extension Number	Select this to allow incoming calls to dial extensions that are not associated with specific key codes on the **Options** list below. Clear it to limit all input to the key codes listed on the **Options** table below.
Forward to a specific extension directly	Select this option to forward all calls that come into this auto-attendant to the specified extension, ACD, page group, hunt group, or user defined number.
Play audio file before forward to a specific extension	Select this option to play the uploaded audio file before forwarding the call to the specified extension, ACD, page group, hunt group, or user defined number.
Operator Settings	
Key	Select either **0** or **9** to be the default operator key. When a caller presses the operator key, his calls is routed to the associated **Extension**.
Extension	Enter an extension number to associate with the operator **Key**. When that key is pressed, the call is routed to this extension.
Action Type	Select how the auto-attendant should proceed if no key is pressed for 5 seconds or the caller inputs an incorrect key code three times in a row. • **Hang Up** disconnects the call. • **Extension** routes the call to the specified extension. • **ACD** engages the ACD system. See Chapter 38 on page 553 for details on this feature. • **Page Group** forwards the call to the page group you specify. See Chapter 37 on page 549 for details on this feature. • **Hunt Group** forwards the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Auto Attendant** forwards the call to the auto attendant you specify. See Chapter 31 on page 503 for details on this feature. • **User Defined Number** forwards the call to the extension or other phone number you specify. Enter a number 3-20 digits in length.
Options	This section displays the actions configured for this auto-attendant menu.
Add Option	Click this to create a new option entry.
Add Child	Select an option entry that displays **sub-menu** as the **Action** and click this to create a sub-entry. See Section 31.3.4 on page 512 for details.
Edit	Select an entry and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Key	This field displays the digits a caller must dial to perform an action.
Action	This field displays the function of an option.
Extension	This field displays either the extension, hunting group or ACD number that this call is forwarded to or it is blank if the action for this auto-attendant option is set to **Forward to a sub menu**. Click **Next Menu** to configure the settings for a sub menu.
Description	This field displays the description for this action.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

31.3.5.1 The Add/Edit Night Service Auto-Attendant Screen

The Add/Edit Night Service Auto-Attendant screen is identical to the Add/Edit Office Hours Auto-Attendant screen. See Section 31.3.3 on page 511 for details.

31.3.6 Greeting

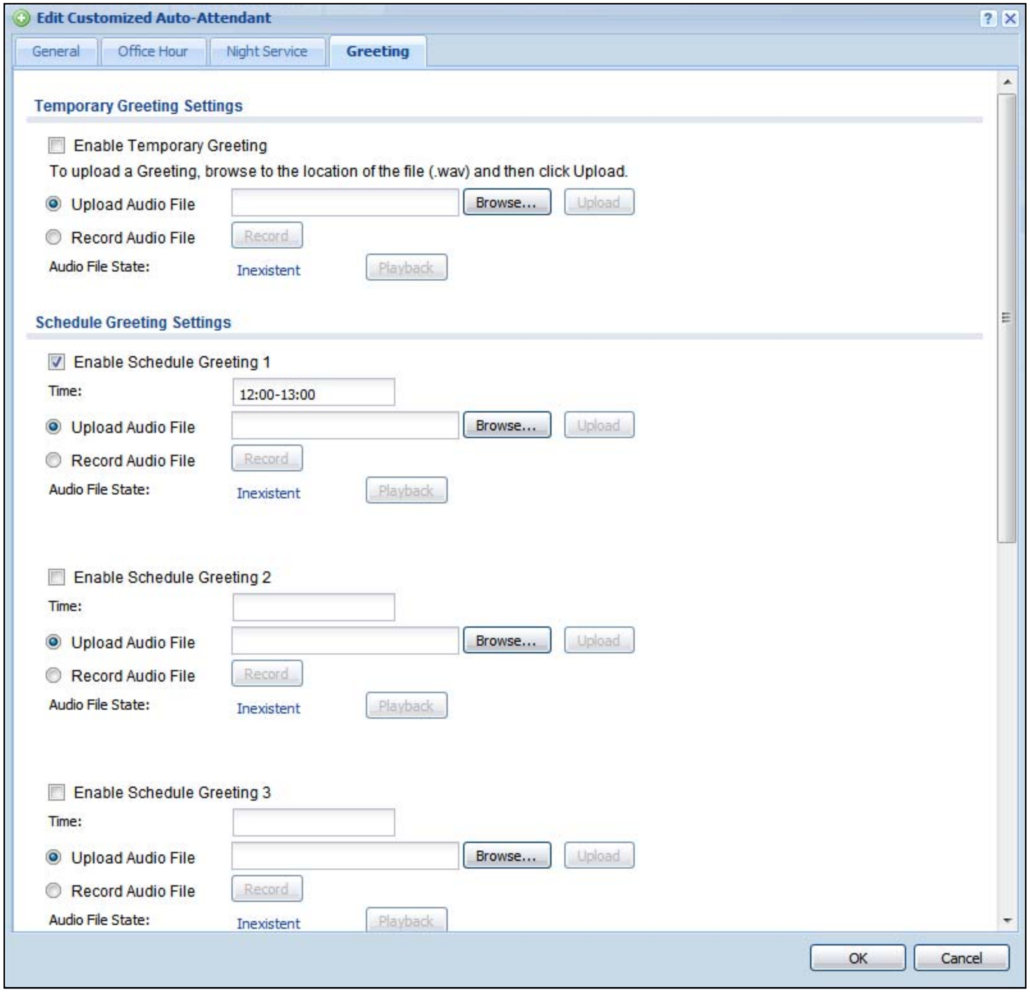
Use this screen to set up custom auto-attendant messages.

The **Temporary Greeting** can be played before the normal auto-attendant greeting. This can be used to broadcast special messages, such as special operating hours for the office building (“We’re sorry but the Acme Mail Order Company is closed today to observe the holiday.”)

The **Schedule Greeting** can be played during specific time range every day. This can be used to broadcast to highlight certain information only at certain hours, such as lunch time hours for the office building (“Thank you for calling the Acme Mail Order Company. As it is currently lunch time, representatives may be unavailable until 1 PM.”)

In the **Configuration** > **PBX** > **Outbound Line Management** > **Auto-Attendant > Customized** screen click the **Add** or **Edit** icon for an item in the auto-attendant list and select the **Greeting** tab to view a screen as shown next.

Figure 335 Greeting Setting



Temporary Greeting Settings

☐ Enable Temporary Greeting

To upload a Greeting, browse to the location of the file (.wav) and then click Upload.

● Upload Audio File

○ Record Audio File

Audio File State: Inexistent

Schedule Greeting Settings

☑ Enable Schedule Greeting 1

Time: 12:00-13:00

● Upload Audio File

○ Record Audio File

Audio File State: Inexistent

☐ Enable Schedule Greeting 2

Time:

● Upload Audio File

○ Record Audio File

Audio File State: Inexistent

☐ Enable Schedule Greeting 3

Time:

● Upload Audio File

○ Record Audio File

Audio File State: Inexistent

Each field is described in the following table.

Table 182 Greeting Setting

LABEL	DESCRIPTION
Temporary Greeting Settings	
Enable Temporary Greeting	Select this to play the temporary greeting immediately before playing the auto-attendant's normal greeting. Clear it to turn this feature off.
Upload Audio File	Click **Browse** to locate an audio file to be used as the temporary auto-attendant greeting message, and **Upload** to copy it to IP-PBX. The audio files you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The total play time of all the AA audio files combined must be less than 30 minutes.
Record Audio File	Click this to record an audio file through the extension set as the recording peer.
Audio File State	This indicates whether an audio file has been uploaded to the ISG50 or not. You can also **Playback** the audio file to hear how it sounds.
Schedule Greeting Settings	
Enable Schedule Greeting 1~6	This indicates the position of the item in the list.
Time	Enter the time range in one of six available fields for this scheduled greeting to be played. Time should be entered using 24-hour notation and the two times separated by a hyphen (hh:mm-hh:mm).
Upload Audio File	Click **Browse** to locate an audio file to be used as the temporary auto-attendant greeting message, and **Upload** to copy it to IP-PBX. The audio files you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The total play time of all the AA audio files combined must be less than 30 minutes.
Record Audio File	Click this to record an audio file through the extension set as the recording peer.
Audio File State	This indicates whether an audio file has been uploaded to the ISG50 or not. You can also **Playback** the audio file to hear how it sounds.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

31.4 Technical Reference

The following section contains additional technical information about the ISG50 features described in this chapter.

How to Record Auto-Attendant Audio Files on Your Computer

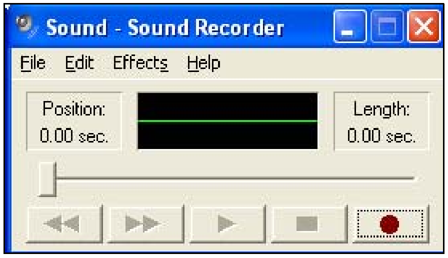
Follow the steps in this section to record audio files on your computer for use by an auto-attendant.

Note: This example uses the components available in the Microsoft Windows 2000 and XP operating system to create the audio files. Windows Vista, Windows 7, Mac OS and Linux users may want to use another program such as Audacity. Use this section as a guideline only.

Note: Make sure you have a microphone connected to your computer or that your system has an internal microphone (and that it is enabled).

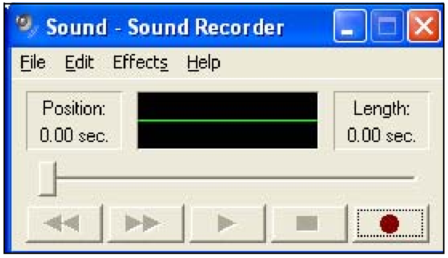
1 Open your sound recording software (Sound Recorder on Windows XP). From your desktop, click **Start > All Programs > Accessories > Entertainment > Sound Recorder**.

Figure 336 Sound Recorder


Sound - Sound Recorder
File Edit Effects Help
Position:
0.00 sec.
Length:
0.00 sec.

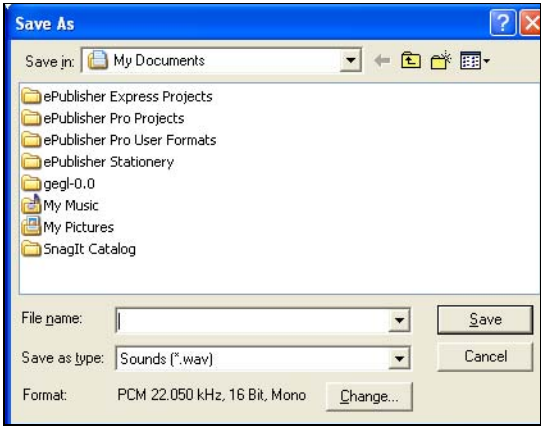
2 Record your audio file. When you are ready to record, click **Record**. When you are finished recording, click **Stop**.

Figure 337 Recording Audio


Sound - Sound Recorder
File Edit Effects Help
Position:
0.00 sec.
Length:
0.00 sec.

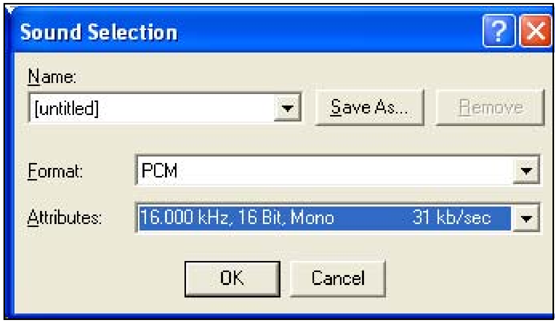
3 Save your audio file. Type a name for the audio file in the **File name:** field and then click **Change** to make sure that the file is saved in the correct format.

Figure 338 Saving Audio Files


Save As
Save in: My Documents
ePublisher Express Projects
ePublisher Pro Projects
ePublisher Pro User Formats
ePublisher Stationery
gegl-0.0
My Music
My Pictures
SnagIt Catalog
File name:
Save
Save as type: Sounds (*.wav)
Cancel
Format: PCM 22.050 kHz, 16 Bit, Mono
Change...

4 Specify the file format. In the **Sound Selection** window. Choose **PCM** in the **Format** field. Next, set the **Attributes to 16,000 kHz, 16 Bit, Mono**. Click **OK** when you are done.

Figure 339 Audio File Settings



Sound Selection
Name:
Save As...
Remove
OK
Cancel

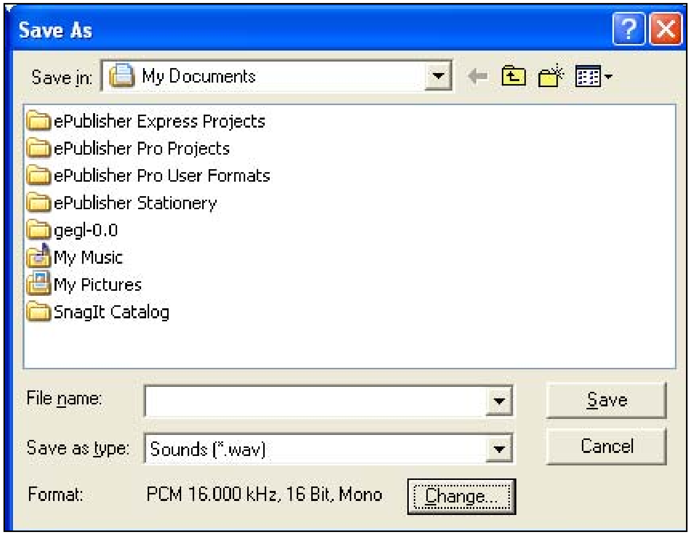
Name: [untitled]

Format: PCM

Attributes: 16.000 kHz, 16 Bit, Mono 31 kb/sec

5 Confirm your settings. Specify a location for the audio file by browsing to a suitable location on your file system. Click **Save** when you are finished.

Figure 340 Confirm File Settings



Save As
Save in:
ePublisher Express Projects
ePublisher Pro Projects
ePublisher Pro User Formats
ePublisher Stationery
gegl-0.0
My Music
My Pictures
SnagIt Catalog
File name:
Save
Cancel
Change...

Save in: My Documents

Save as type: Sounds (*.wav)

Format: PCM 16.000 kHz, 16 Bit, Mono

32

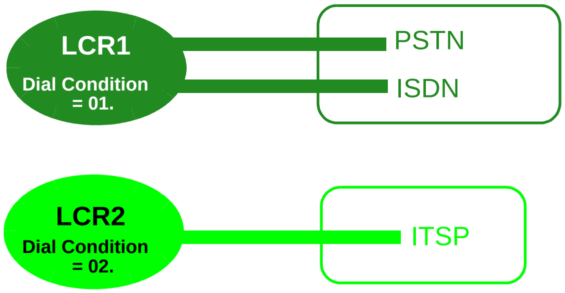
LCR

32.1 Overview

This chapter shows you how to configure dialing rules, also referred to as LCR (Least Cost Routing) on the ISG50.

The following figure shows an example of two LCRs. **LCR1** is composed of outbound line groups **PSTN** and **ISDN** along with the dial condition **01.** (the period (**.**) is part of the dial condition). **LCR2** is composed of outbound line group **ITSP** along with the dial condition **02.**. When a user calls “021234” the call is routed through the outbound line group defined in **LCR2**.

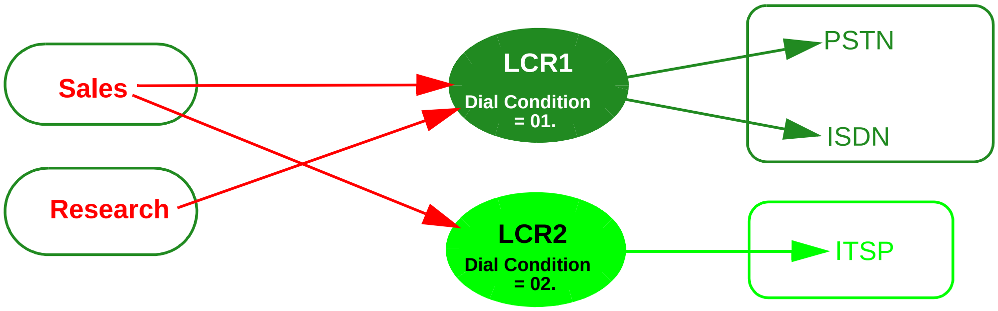
Figure 341 LCR Components Example



When an LCR contains more than one outbound line group, as in the **LCR1** example, the administrator can prioritize the outbound line groups in the LCR. When a call is made using an LCR with multiple outbound line groups, the ISG50 tries to use the higher priority outbound line group first and, if the line is not available, then it tries a lower priority outbound line group.

The following figure shows a possible assignment of LCRs to authority groups. In our example, the **Sales** authority group has been associated with both **LCR1** and **LCR2**, so extensions that are part of **Sales** can use any outbound line group they choose. The second authority group - **Research**, only has **LCR1** assigned to it, so extensions that are part of **Research** cannot use outbound line group **ITSP**.

Figure 342 LCR Components Example



32.1.1 What You Can Do in this Chapter

Use the **LCR** screen to configure settings for your dialing rules for outbound calls routing. See Section 32.2 on page 521.

32.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

LCR

LCRs are made up of two components. The first part of an LCR is a set of 1 or more outbound line groups (see Chapter 30 on page 477). The second part of an LCR is a set of dial conditions, or a set of pattern of digits that distinguish each individual LCR.

LCRs define which outbound line group(s) that authority groups, trusted SIP peers or outbound line groups can use to make an outgoing call. This is done via group management, see Chapter 33 on page 526. Once you create an LCR, you can associate it with:

- **Authority Groups** - give all the extensions contained in an authority group the right to use the outbound line groups configured in the LCR.
- **Trusted SIP Peers** - give the telephones connected to the SIP peer the right to call the ISG50 and then dial out from the ISG50 using the outbound line groups configured in the LCR.
- **Outbound Line Groups** - give anyone calling in via the associated outbound line group the right to use the ISG50 to make calls via the outbound line groups configured in the LCR.

Outbound Line Group

The outbound lines define a connection between the ISG50 and PSTN, ISDN, ITSP or your trusted peer. See Section 30.1 on page 477 for more information.

32.1.3 Before You Begin

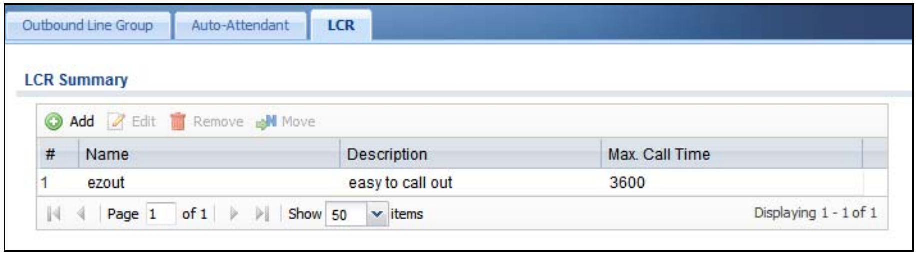
Before you start to configure an LCR, please consider the following.

- You have to define your outbound dialing plan. For example, dial a number starting with “0” is for local calls, “200” is for international calls, “3” is a call to branch office, etc.
- You should define at least one outbound line group. See Section 30.2 on page 481.

32.2 LCR

Use this screen to view outbound dialing rules (LCRs) configured on the ISG50. To access this screen, click **Configuration** > **PBX** > **Outbound Line Management** > **LCR**.

Figure 343 Configuration > PBX > Outbound Line Management > LCR



#	Name	Description	Max. Call Time
1	ezout	easy to call out	3600

Each field is described in the following table.

Table 183 Configuration > PBX > Outbound Line Management > LCR

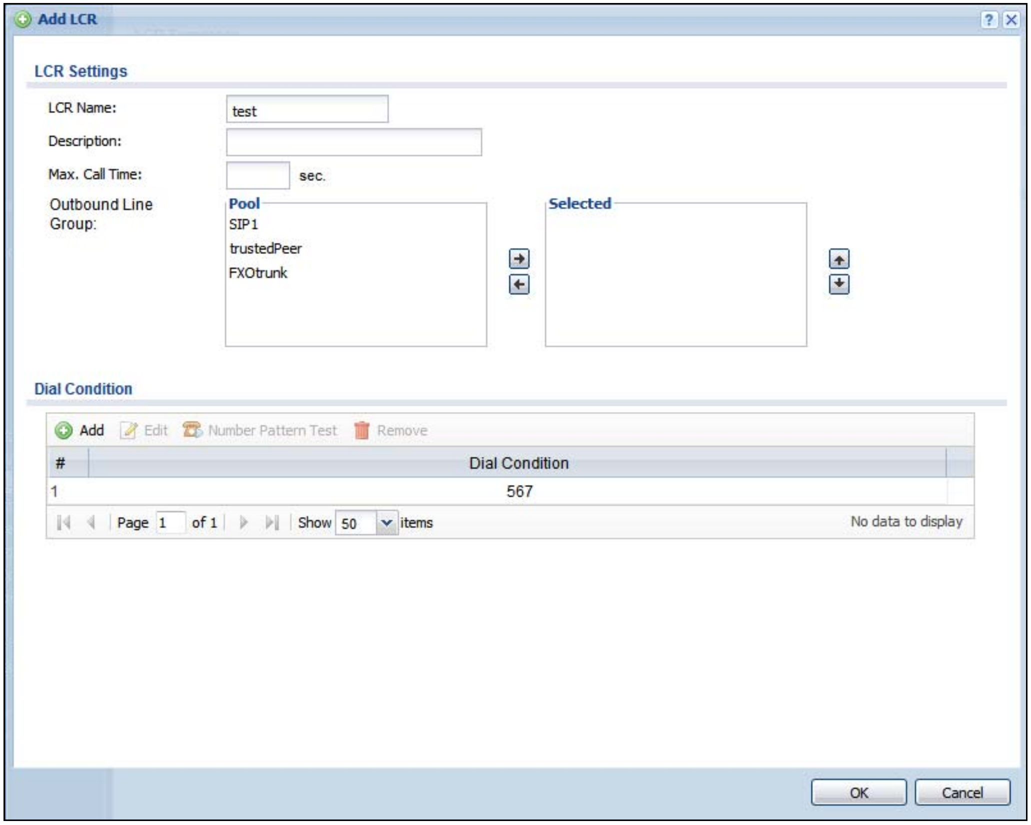
LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry.
Remove	To remove one or more entries, select them and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Move	To change a dialing rule’s position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This is the position of your dialing rule in the global rule list. The ordering of your rules is important as rules are applied in sequence.
Name	This is the name of the LCR.
Description	This text describes the LCR.

32.2.1 LCR Configuration

Use this screen to choose the outbound line groups and create dialing conditions for an LCR. To access this screen, click the **Add** or **Edit** icon in the **Dial Condition List** section of the **LCR** screen to view the screen as shown.

Note: Only the **Add LCR** screen is shown. In the **Edit LCR** screen, some of the fields are read-only. Before you configure any dial conditions for an LCR, you must first configure a name for the LCR.

Figure 344 Configuration > PBX > Outbound Line Management > LCR > Add



LCR Name: test

Description:

Max. Call Time: sec.

Outbound Line Group: Pool: SIP1, trustedPeer, FXOtrunk; Selected:

#	Dial Condition
1	567

Page 1 of 1 | Show 50 items | No data to display

Each field is described in the following table.

Table 184 Configuration > PBX > Outbound Line Management > LCR > Add

LABEL	DESCRIPTION
LCR Settings	
LCR Name	Type a short name to identify this outbound dialing rule (LCR). You can use letters “a-z”, “A-Z”, numbers “0-9” and the underscore “_” character. Spaces are not allowed. The first character cannot be a digit.
Description	Type a short description for this outbound dialing rule (LCR). You can use printable ASCII characters; spaces are allowed.
Max. Call Time	Leave this field blank, if you don’t want to limit the duration of outgoing calls that use this outbound dialing rule (LCR). Alternatively, enter the number of seconds (1-99999) to which you want to limit the duration of outgoing calls that use this outbound dialing rule (LCR).

Table 184 Configuration > PBX > Outbound Line Management > LCR > Add (continued)

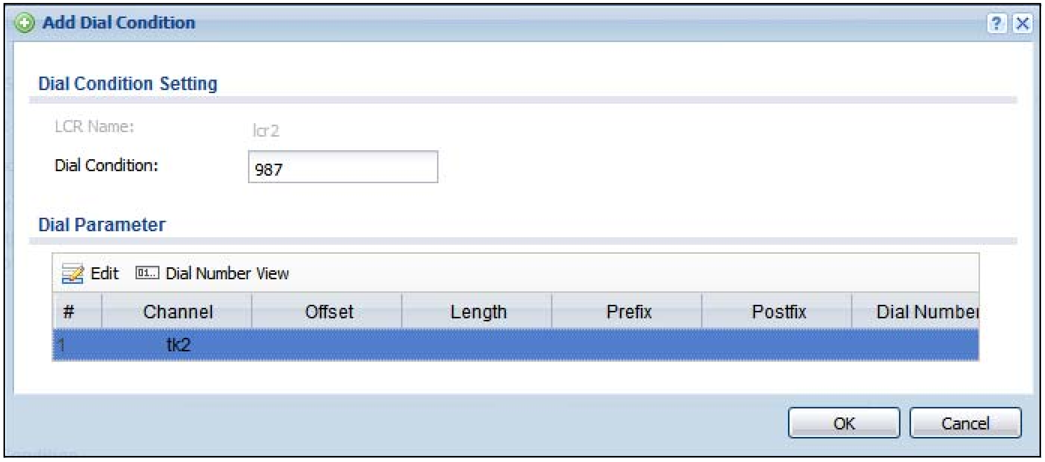
LABEL	DESCRIPTION
Outbound Line Group	Use this section to add or remove outbound line groups from this outbound dialing rule (LCR). • Add an outbound line group to this LCR: Highlight an outbound line group in the **Pool** column by clicking on it and then click the **Right** button to move it to the **Selected** column. • Remove an outbound line group from this LCR: Highlight an outbound line group in the **Selected** column by clicking on it and then click the **Left** button to move it to the **Pool** column. If the LCR contains multiple outbound line groups, you can use the **Up** and **Down** buttons to specify the priority of the outbound line groups. • Highlight an outbound line group in the **Selected** column by clicking on it and then click the **Up** button to raise its priority. • Highlight an outbound line group in the **Selected** column by clicking on it and then click the **Down** button to lower its priority.
Dial Condition	
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Number Pattern Test	Select a dial condition parameter entry and click **Number Pattern Test** to check whether a number dialed from one of the extensions meets the criteria specified in the **Dial Condition** field. In the pop-up window, type a number in the **Number Pattern Test** field and click the right arrow button. An **O** appears, if the number you typed matches the dial condition. An **X** appears, if the number you typed does not match the dial condition.
Remove	To remove one or more entries, select them and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Dial Condition	This field displays the dial conditions (string of digits) that are used by this outbound dialing rule (LCR).
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

32.2.2 Add/Edit LCR Dial Condition

Use this screen to set up a dialing condition for an LCR. To access this screen, click the **Add** or **Edit** icon in the **Dial Condition List** section of the **LCR** screen you are configuring to view a screen as shown.

Note: Only the **Add Dial Condition** screen is shown. In the **Edit Dial Condition** screen, some of the fields are read-only.

Figure 345 Configuration > PBX > Outbound Line Management > LCR > Add > Add



LCR Name: lcr2

Dial Condition: 987

#	Channel	Offset	Length	Prefix	Postfix	Dial Number
1	tk2					

Each field is described in the following table.

Table 185 Configuration > PBX > Outbound Line Management > LCR > Add > Add

LABEL	DESCRIPTION
LCR Name	This field displays the name of the outbound dialing rule that this dialing condition applies to.
Dial Condition	Create the criteria for using this outbound dialing rule. The criteria can be • a specific number - for example “55555555”; in this case the number dialed by users must match this string exactly. • any number starting with a specified pattern of digits - for example “0.”, “555.”, “011.” and so on; in this case the number dialed must match the digits before the period “.” and it doesn’t matter what follows. For example dialing “0222-2222” matches the dialing condition “0.”. You can also specify a range for digits within a dial condition. You can: • use the letters **X**, **Z**, **N** to specify a range of numbers to match. **X** represents the range **0**-**9**, **Z** represents the range **1**-**9** and **N** represents the range **2**-**9**. • use brackets to specify an allowed range for a dialed digit. For example **[0-8]** or **[0-46-9]**, in the second example **5** is not allowed. Use the **Right** button to test if the dial condition is in acceptable format. Note: You should make sure to create unique dial conditions for each LCR. The ISG50 is not able to distinguish between LCRs if they have the same dial condition.
Dial Parameter	Use this section to configure what the ISG50 does with the phone numbers this LCR sends to this outbound line group.
Edit	Double click the entry or select it and click **Edit** to modify it.
Dial Number View	Click this to display the phone number the ISG50 has the outbound line group send for the number in the **Dial Number** field.
#	This field displays the index number of a dial parameter.
Channel	This column identifies the outbound line groups for this outbound dialing rule (LCR).
Offset	Specify how many initial digits of the dialed number should not be included in the number going out of the ISG50.
Length	Specify whether the number dialed should be limited in length. If you set a limit, the ISG50 cuts off numbers which extend beyond the limit.

Table 185 Configuration > PBX > Outbound Line Management > LCR > Add > Add (continued)

LABEL	DESCRIPTION
Prefix	Specify a number which should be inserted at the beginning of the dialed number before it is sent out from the ISG50.
Postfix	Specify a number which should be appended to the end of the dialed number before it is sent out from the ISG50.
Dial Number	This field displays the number to which a dial parameter applies.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

33

Group Management

33.1 Overview

This chapter shows you how to manage the ISG50's authority groups and outbound line groups.

Group management allows you to control the types of calls made via the ISG50. See the following figure for what you can configure in the group management.

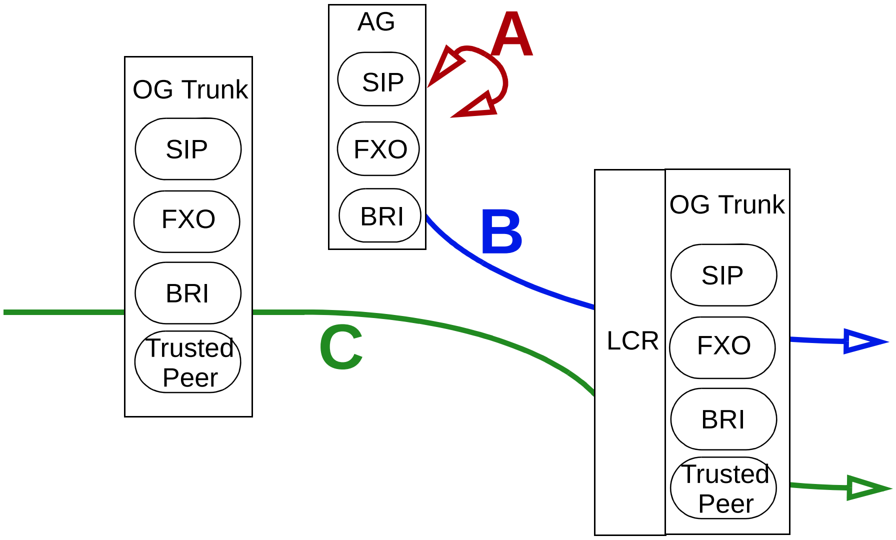
A - You can allow or disallow an extension group (defined in the authority group, AG) to call extensions in the same extension group or other extension groups.

B - You can manage the types of outgoing calls that extensions within authority groups can make.

C - You can manage incoming calls that callers from outside your organization can make using different interfaces.

You grant calling rights by creating associations or links between the various logical entities configured on the ISG50.

Figure 346 Group Management Example



The following sections give an overview of granting calling rights to authority groups (see Managing Authority Groups on page 527), followed by granting calling rights to outbound line groups (see Managing Outbound Line Groups on page 528).

33.1.1 What You Can Do in this Chapter

Use the **Group Management** screens to view and manage the associations for the authority and outbound line groups configured on the ISG50. See Section 33.2 on page 530.

33.1.2 What You Need to Know

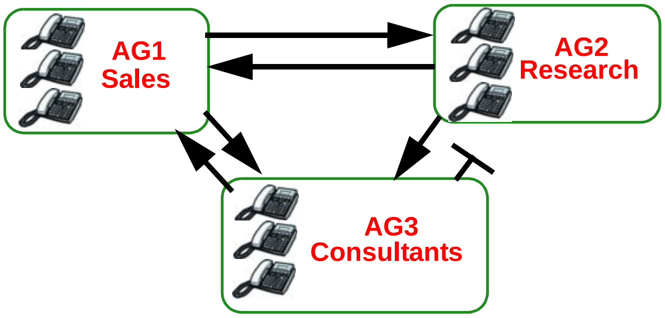
The following terms and concepts may help you as you read through the chapter.

Managing Authority Groups

You control extensions within an authority group by associating (linking) authority groups with:

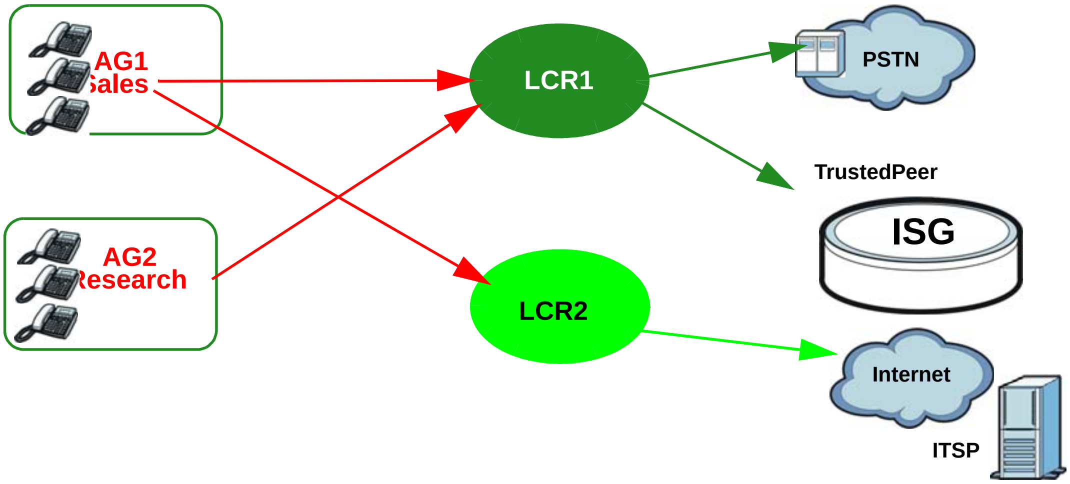
- **Other Authority Groups** - When you create an authority group it is by default linked to all other authority groups created on the ISG50 and all the other authority groups are also linked to it. This means that any extension created on the ISG50 can call any other extension created on the ISG50 regardless if they are part of the same authority group. You can, however, stop extensions within one authority group from calling extensions in another authority group. An example is shown below. You have an organization with three authority groups (AG1-AG3). You can remove the link from one authority group (for example AG3) to another authority group (for example AG2) to stop extensions in AG3 from calling AG2 (AG2 can still call AG3).

Figure 347 Group Management - Authority Group to Authority Group



- **LCRs** - An LCR is an outbound dialing rule. When you create links from an authority group to an LCR, you allow the extensions in that authority group to make outbound calls via the outbound line groups configured in the LCR. The following figure shows **AG1**, which is an authority group for the sales department, associated with LCR1 (this could be an LCR allowing calls through your local telephone service provider - **PSTN** and calls via a link to your branch office - **TrustedPeer**) and LCR2 (this could be an LCR for long distance calls via your VoIP service provider **ITSP**). **AG2** is associated with **LCR1** only. In this case extensions belonging to **AG1** can make calls via all outbound line groups, whereas extensions in **AG2** are limited to calls to your local telephone company and your branch office.

Figure 348 Group Management - Authority Group to LCR



Managing Outbound Line Groups

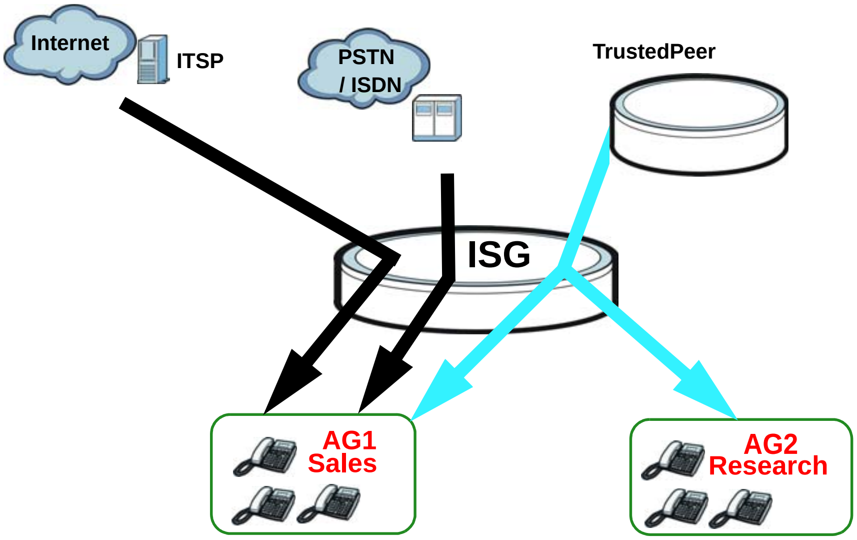
Outbound line groups include SIP, FXO, ISDN BRI Trunks, and Trusted Peers as defined in Chapter 30 on page 477. For management purposes the ISG50 grants rights to calls coming in via these channels based on the outbound line group they are part of. You can manage incoming calls by associating (linking) outbound line groups with:

- **Authority Groups** - When you create an outbound line group it is by default linked to all authority groups created on the ISG50. This means that calls coming in via this outbound line group are authorized to call any extension created on the ISG50. You can remove the link from an outbound line group to an authority group to stop incoming calls from an outbound line group from going to a specific authority group.

Note: You must also configure auto-attendant settings before calls coming in from outside lines can call the extensions created on the ISG50. See Chapter 31 on page 503.

The following example shows a configuration with three outbound line groups. **ITSP** represents a SIP trunk to your VoIP service provider. **PSTN** represents a link to your local traditional telephone service provider and **TrustedPeer** is a connection to your branch office. Incoming calls from **ITSP** and from **PSTN** are allowed to only reach extensions of your sales team (**AG1**). Calls coming in from **TrustedPeer** are allowed to reach the extensions of both the sales (**AG1**) and research (**AG2**) departments. This configuration is accomplished by removing the association to **AG2** from the **ITSP** and **PSTN** outbound line groups.

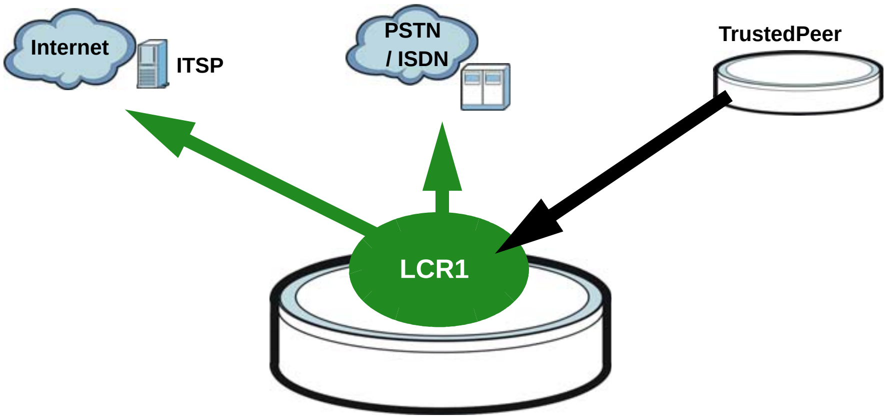
Figure 349 Group Management - Outbound Line Group to Authority Group



- **LCRs** (LCR is the outbound dialing rule) - When you create links from an outbound line group to an LCR, you allow incoming calls from that outbound line group to make outbound calls via the outbound line groups configured in the LCR. For example, someone calling from outside your organization can use the ISG50 to forward their call to another outside line.

  In the following example, outbound line group **TrustedPeer** is associated with **LCR1**. **LCR1** is comprised of two outbound line groups: a SIP trunk to your VoIP service provider - **ITSP** and a connection to your local traditional telephone company - **PSTN / ISDN**. Calls coming in via the **TrustedPeer** connection can use the **ITSP** and **PSTN / ISDN** connections to complete their calls.

Figure 350 Group Management - Outbound Line Group to LCR



33.1.3 Before You Begin

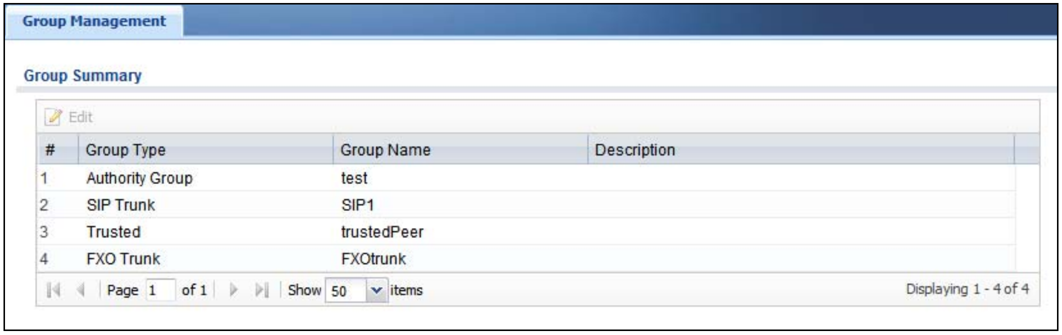
Before you start to configure a group management, you need to do the following.

- Configure authority group(s). See Section 29.2 on page 458.
- Configure outbound line group(s) and the corresponding auto-attendant settings. See Section 30.2 on page 481.

33.2 Group Management Screen

Use this screen to view and manage the associations for the authority and outbound line groups configured on the ISG50. To access this screen, click **Configuration > PBX > Group Management**.

Figure 351 Configuration > PBX > Group Management



#	Group Type	Group Name	Description
1	Authority Group	test	
2	SIP Trunk	SIP1	
3	Trusted	trustedPeer	
4	FXO Trunk	FXOtrunk	

Each field is described in the following table.

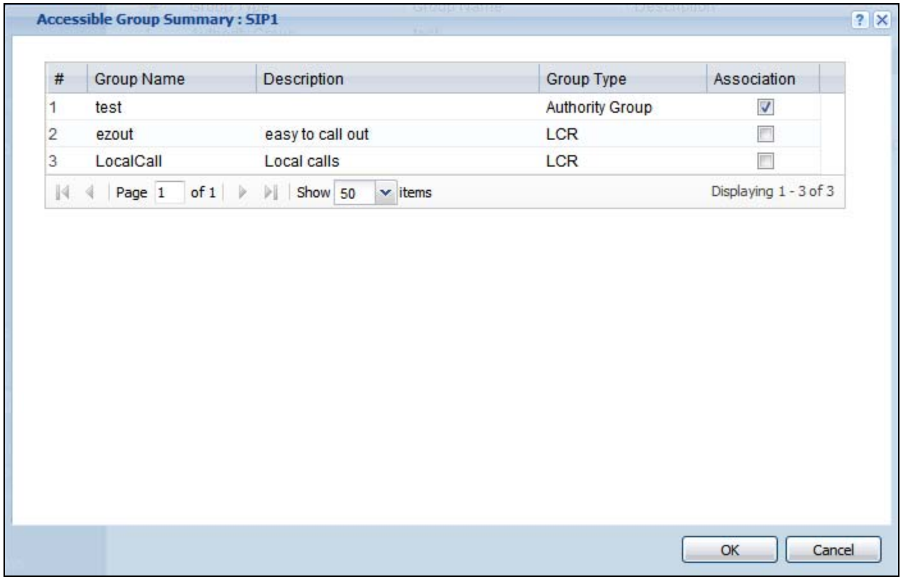
Table 186 Configuration > PBX > Group Management

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
#	This field is a sequential value, and it is not associated with a specific entry.
Group Type	This is the type of group on the ISG50 to which this entry belongs: • **Authority Group** - These are the authority groups containing extensions on the ISG50. • **SIP Trunk** - These are outside lines to a SIP server at your VoIP service provider. • **Trusted** - These are outside lines to another SIP server (for example another ISG50) that has configured your ISG50 as a trusted peer. • **FXO Trunk** - These are outside lines via the FXO ports on the ISG50. • **BRI Trunk** - This refers to a connection from the ISG50 to the basic rate ISDN trunk line via the BRI port on the ISG50.
Group Name	This field displays the name of a group (authority group or an outbound line group).
Description	This field displays the description of this group.

33.2.1 Edit Group Management Associations

Use this screen to configure links from an authority group or an outbound line group to authority groups, or LCRs configured on the ISG50. To access this screen, select the group you want to configure in the **Configuration > PBX > Group Management** screen and click **Edit**.

Figure 352 Configuration > PBX > Group Management > Edit



#	Group Name	Description	Group Type	Association
1	test		Authority Group	☑
2	ezout	easy to call out	LCR	☐
3	LocalCall	Local calls	LCR	☐

Each field is described in the following table.

Table 187 Configuration > PBX > Group Management > Edit

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Group Name	This field displays the name of an authority group or LCR to which you can configure a link.
Description	This field displays the description of the group to which you can create a link.
Group Type	This field identifies whether you are creating a link to: **Authority Group** - another set of extensions on the ISG50. **LCR** - an outbound dialing rule containing outbound line groups.
Association	Select this to link a group you are configuring to another group. Clear it to remove a link between the group you are configuring and another group.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

34

Call Services

34.1 Overview

This chapter shows you how to configure and use call services on the ISG50. There are a variety of call services that can be configured.

34.1.1 What You Can Do in this Chapter

- Use the **Auto Callback** screen to configure the ISG50 to automatically call an extension once it becomes available (ends an existing conversation). This eliminates the need for you to keep trying to call a busy extension. See Section 34.2 on page 533.
- Use the **Call Park** screen to configure the ISG50 to allow users to put a call on hold at one extension and pick up the call from another extension in your organization. See Section 34.3 on page 534.
- Use the **Call Waiting** screen to configure the ISG50 to allow users to put a call on hold at one extension and pick up another incoming call. See Section 34.4 on page 536.
- Use the **Emergency Call** screen to configure emergency numbers, which the ISG50 treats with the highest priority. Even if all outbound lines from the ISG50 are busy, the ISG50 will drop an existing FXO channel and allow an emergency call to complete. See Section 34.5 on page 538.
- Use the **Music on Hold** screen to upload your choice of audio to play while callers are placed on hold. See Section 34.6 on page 539.
- Use the **Call Transfer** screen to configure the ISG50 to allow users to transfer an incoming call that they have answered to another extension in your organization. See Section 34.7 on page 541.
- Use the **Call Block** screen to configure the black list settings which is not allowed to call into your ISG50. See Section 34.8 on page 542.

34.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

About Emergency Calls and VoIP

In the past, many commercial VoIP phone services have lacked the ability to deal correctly with emergency calls. Such VoIP services have been unable either to connect emergency calls to an emergency dispatcher (at a Public Safety Answering Point, or PSAP), or to adequately provide information on the caller’s whereabouts to the dispatcher.

For this reason, the FCC (the Federal Communications Commission of the United States) has imposed “Enhanced 911” (E911) obligations on providers of “interconnected VoIP” services. Interconnected VoIP services are those that, in addition to making calls over the Internet, also connect to the regular public telephone network. E911 systems not only route emergency calls made from VoIP accounts to emergency dispatchers, but also provide information on the call's originating number and, usually, location information.

However, this system still has disadvantages over traditional emergency call service. For example, the physical location provided to the PSAP is usually the account-holder's address as registered with the VoIP provider; this is not necessarily the location from which the VoIP account is being used. Furthermore, VoIP emergency calls are subject to the limitations of the Internet connection over which they are made, which may be unreliable. Also, VoIP services that do not directly connect to the public telephone network are not required to adhere to the FCC's E911 regulations. Lastly, the E911 service is available only in North America. Similar systems exist elsewhere in the world, but regulation and implementation may vary.

For these reasons, the ISG50 routes all calls made to the emergency numbers you configure via its FXO interface whenever possible. The ISG50 drops an ongoing FXO call if necessary.

34.1.3 Before You Begin

Emergency Calls

Before you configure emergency calling, ensure that you are aware of all local emergency call numbers used in the location where the ISG50 is to operate. Bear in mind that emergency calls may be made to phone numbers other than the standard public emergency services number (to a private security company or medical facility, for example).

Music on Hold

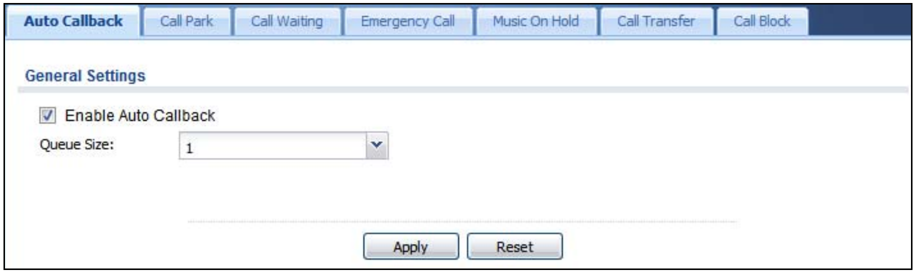
Before you configure music on hold, ensure that the audio file you want to use is compatible with the standards described in Section 34.6 on page 539.

34.2 The Auto Callback Screen

The auto callback feature is used when a caller encounters a busy signal when dialing one of the extensions. The caller can then request the ISG50 to automatically call both parties when both of the extensions are free.

Click **Configuration > PBX > Call Service > Auto Callback** to configure the auto callback feature.

Figure 353 Configuration > PBX > Call Service > Auto Callback



☑ Enable Auto Callback

Queue Size: 1

The following table describes the labels in this screen.

Table 188 Configuration > PBX > Call Service > Auto Callback

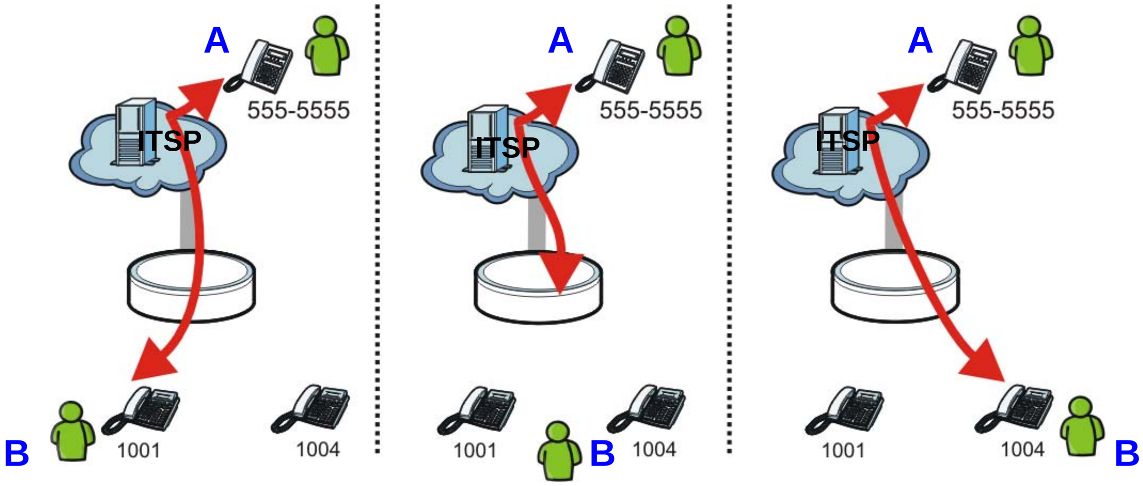
LABEL	DESCRIPTION
Enable Auto Callback	Select this to activate the auto callback feature. Note: To enable auto callback, the personal auto-attendant for internal calls must also be enabled. See Section 27.2 on page 431.
Queue Size	Select a limit to the number of auto callback requests for each extension.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

34.3 The Call Park Screen

Call parking is similar to placing a call on hold. The difference is that you can pick the call up again from another telephone extension in your organization.

The ISG50 allows you to configure a representative extension for a call parking lot. The parking lot places a call in parking slot and informs you of the parking slot number that you can use to reconnect to the parked call. You can reconnect to the call from any extension within your organization. The following figure shows the progression of call parking.

Figure 354 Call Parking Overview



A step by step progression is the following

Table 189 Call Parking Progression

CALLER A	ISG50	CALLER B
1. Caller A makes a call to caller B.	2. The ISG50 routes the call to caller B at extension 1001.	3. Caller B picks up the call.
Conversation between caller A and B		
		4. Caller B transfers the call to the representative extension.

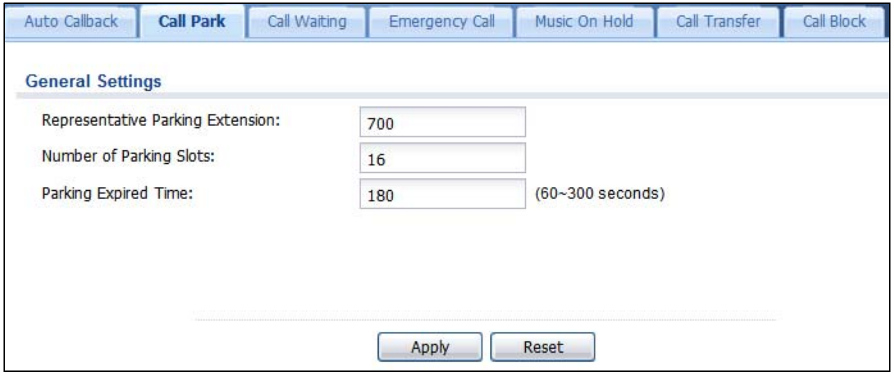
Table 189 Call Parking Progression

CALLER A	ISG50	CALLER B
	5. The ISG50 parks the call and informs caller B of the number to call to reconnect to the call. This is called the parking slot number.	
		6. Caller B walks to another extension and reconnects to the call with A by dialing the parking slot number.
Conversation between caller A and B continues		

34.3.1 Configuring the Call Park Screen

Use this screen to configure call parking on the ISG50. Click **Configuration > PBX > Call Service > Call Park** to open the screen.

Figure 355 Configuration > PBX > Call Service > Call Park



Representative Parking Extension: 700
Number of Parking Slots: 16
Parking Expired Time: 180 (60~300 seconds)

The following table describes the labels in this screen.

Table 190 Configuration > PBX > Call Service > Call Park

LABEL	DESCRIPTION
Representative Parking Extension	Enter the telephone number users should dial to park a telephone call. You can use 3-8 digits.
Number of Parking Slots	Enter the total number of call parking slot extensions to make available. This also establishes the range of numbers that users will have to dial to retrieve a parked call. You can use 1-99 positions.
Parking Expired Time	Enter the maximum number of seconds that a call can be parked. After a parked call exceeds this amount of time, it will ring back to the extension that parked the call. The range you can use is 60-300 seconds.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to set every field in this screen to its last-saved value.

34.4 The Call Waiting Screen

Call waiting allows you to put a present call on hold and answer a new call. When a second call comes in, the ISG50 sends a beep tone to you. You can decide to ignore it or to switch to the second call using one of the following methods.

- press the flash button on your telephone
- very quickly press and release the on-hook switch on your telephone

You can switch back to the first call using the same methods above. When you hang up one call, the ISG50 sends you a ring tone if another call is still waiting.

Note: This feature only applies to extension receivers which use SIP or analog phones.

The following figure shows how call waiting works.

Figure 356 Call Waiting Overview

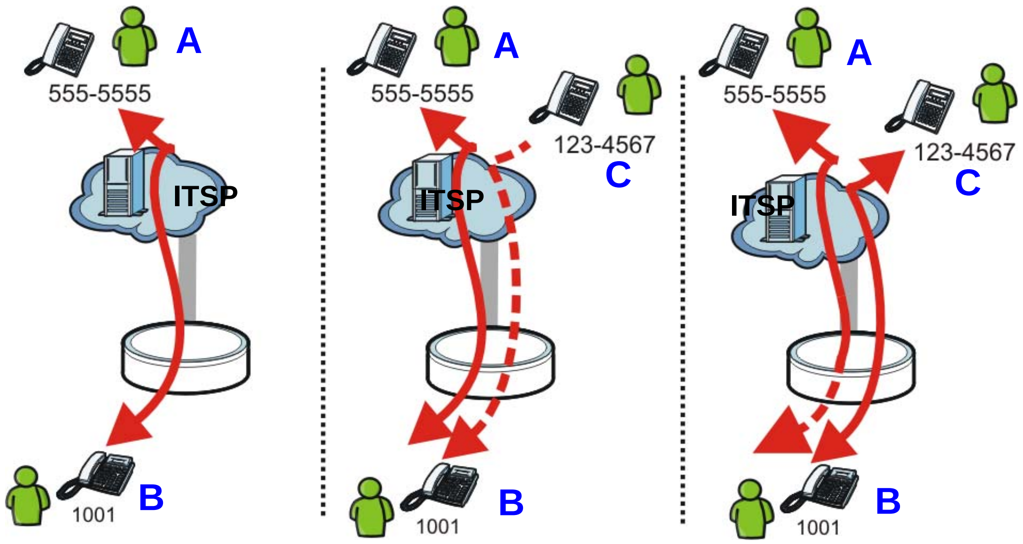


Table 191 Call Waiting Example

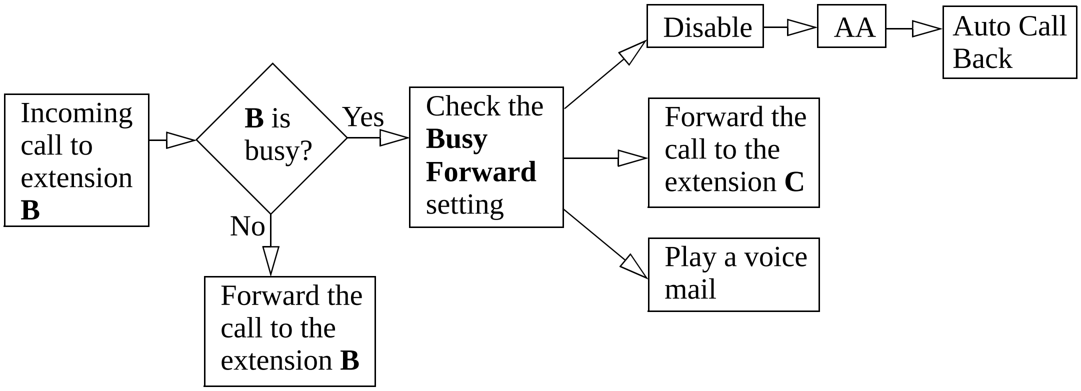
CALLER A	CALLER C	ISG50	RECEIVER B
1. Caller **A** makes a call to caller **B**.		2. The ISG50 routes the call to **B** at extension 1001.	3. **B** picks up the call.
4. Conversation established between caller **A** and **B**			
	5. Caller **C** makes a call to caller **B**.	6. The ISG50 routes the call to **B** at extension 1001.	7. **B** hears a beep tone and decides to answer the second call. **B** then presses the flash button on his telephone).
8. Conversation established between caller **C** and **B**. Caller **A** is on hold. **B** is busy.			

However, for extensions for which you do not enable the call waiting feature, the following happens.

Table 192 No Call Waiting Example

CALLER A	CALLER C	ISG50	RECEIVER B
1. Caller A makes a call to caller B.		2. The ISG50 routes the call to B at extension 1001.	3. B picks up the call.
4. Conversation between caller A and B. Then B is busy.			
	5. Caller C makes a call to caller B.	6. The ISG50 routes the call to B at extension 1001.	7. B replies with a busy tone.
		8. The ISG50 handles the call (from C) by following extension B's **Busy Forward** setting.	

Figure 357 The Flow to Check Whether The Receiver Is Busy Or Not

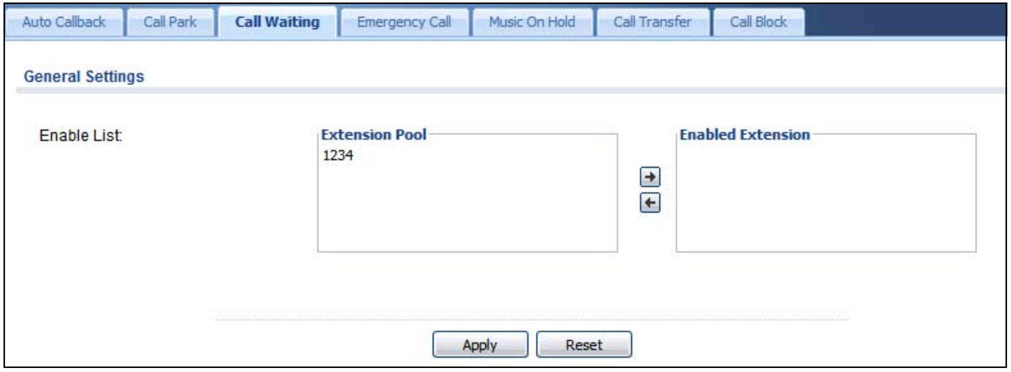

Incoming call to extension **B**
B is busy?
Yes
No
Check the **Busy Forward** setting
Disable
AA
Auto Call Back
Forward the call to the extension **C**
Play a voice mail
Forward the call to the extension **B**

When **B** is busy, additional calls will hear a busy tone and then the ISG50 will handle the calls according to what you configured in the **Busy Forward** setting configured in the extension's **Call Forward** screen for the extension number (see Section 29.3.2 on page 463).

34.4.1 Configuring the Call Waiting Screen

Use this screen to configure call waiting on the ISG50. Click **Configuration > PBX > Call Services > Call Waiting** to open the screen as following.

Figure 358 Configuration > PBX > Call Service > Call Waiting


Auto Callback
Call Park
Call Waiting
Emergency Call
Music On Hold
Call Transfer
Call Block
Apply
Reset

General Settings

Enable List

Extension Pool
1234

Enabled Extension

The following table describes the labels in this screen.

Table 193 Configuration > PBX > Call Service > Call Waiting Setting

LABEL	DESCRIPTION
Extension Pool / Enabled Extension	Call waiting applies to the extensions you move to the **Enabled Extension** list. To add an extension, select it in the **Extension Pool** field and click the **Right** button (to add it into the **Enabled Extension** list). You can remove extensions from the enabled list by selecting them and clicking the **Left** button.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to set every field in this screen to its last-saved value.

34.5 The Emergency Call Screen

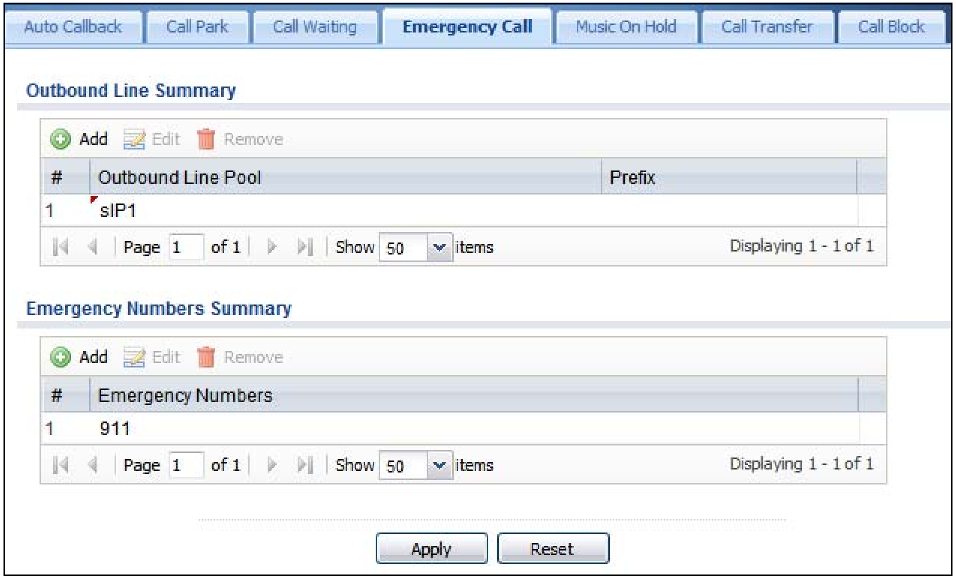
The ISG50 allows you to specify and give higher priority to emergency calls to emergency services. You can configure a list of emergency phone numbers, for example police or fire department, on the ISG50. The ISG50 recognizes when an emergency number is dialed and tries to send the call to the configured destination number. If all the lines on the ISG50 are busy, the ISG50 frees up a line by hanging up an existing conversation and then passing the emergency call to the destination number.

An FXO or BRI outside line has higher priority than a SIP trunk for emergency call use.

34.5.1 Configuring the Emergency Call Screen

Click **Configuration > PBX > Call Service > Emergency Call** to view the following screen.Use this screen to manage emergency call numbers on the ISG50.

Figure 359 Configuration > PBX > Call Service >Emergency Call


Auto Callback
Call Park
Call Waiting
Emergency Call
Music On Hold
Call Transfer
Call Block
Outbound Line Summary
Add
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Emergency Numbers Summary
Add
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Apply
Reset

#	Outbound Line Pool	Prefix
1	sIP1	

#	Emergency Numbers
1	911

The following table describes the labels in this screen.

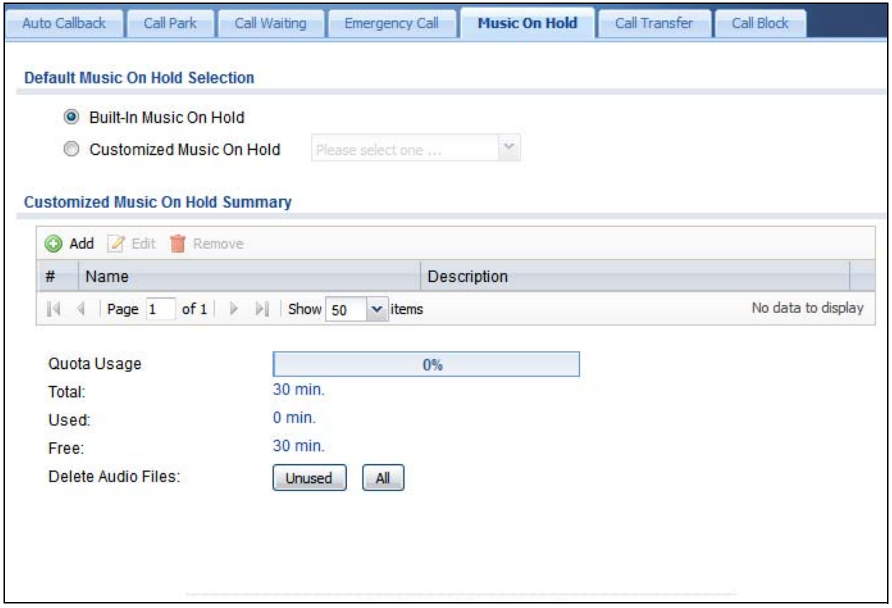
Table 194 Configuration > PBX > Call Service > Emergency Call

LABEL	DESCRIPTION
Outbound Line Summary	Use this section to specify which outside line groups should be used for emergency calls.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field displays the number of the entry.
Outbound Line Pool	This field shows an outside line group selected for emergency call use. When adding or editing an entry, click in the field and use the drop-down list to select an outside line group for emergency call use.
Prefix	This is any prefix that must be added to emergency calls when using this outside line. Specify a number which should be inserted at the beginning of the dialed number before it is sent out from the ISG50. For example, if the ISG50 is behind another PBX and calls to the outside require a “0” to be dialed first, specify it here. When adding or editing an entry, click in the field and type the prefix number necessary to connect users to an emergency number by simply dialing the emergency number you configure in the **Emergency Number Summary** section of this screen.
Emergency Numbers Summary	Use this section to add, edit or remove emergency numbers.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Emergency Numbers	This column displays the emergency numbers currently configured on the ISG50. When adding or editing an entry, click in the field and type the emergency number. This is the number (such as 911) a person dials in case of emergency.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

34.6 The Music on Hold Screen

The ISG50 allows you to specify a music file to play when callers are placed on hold. This lets the callers know that they are still connected. Use this screen to customize the default music callers will hear when placed on hold. If you create any custom profiles then they can override this setting.

Click **Configuration > PBX > Call Service > Music On Hold** to open the screen as shown.


Auto Callback
Call Park
Call Waiting
Emergency Call
Music On Hold
Call Transfer
Call Block
Default Music On Hold Selection
Customized Music On Hold Summary
Add
Edit
Remove
#
Name
Description
Page 1 of 1
Show 50 items
No data to display
Unused
All

● Built-In Music On Hold
○ Customized Music On Hold Please select one ...

Quota Usage 0%
Total: 30 min.
Used: 0 min.
Free: 30 min.
Delete Audio Files: Unused All

Figure 360 Configuration > PBX > Call Service > Music On Hold:

The following table describes the labels in this screen.

Table 195 Configuration > PBX > Call Service > Music On Hold

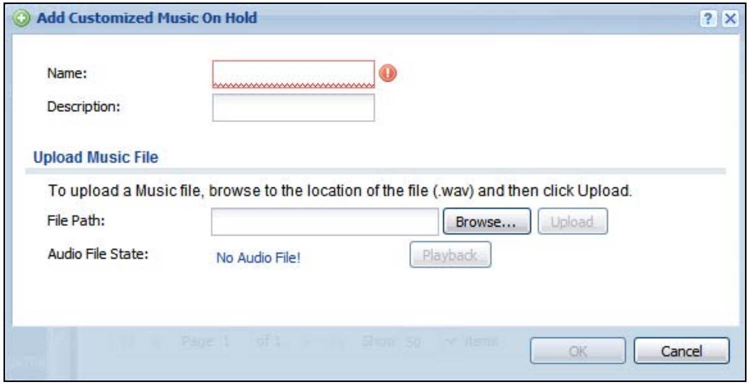
LABEL	DESCRIPTION
Default Music On Hold Selection	Select a music on hold profile to use as the system default. Use either the built-in music on hold profile or a customized music on hold profile that you created.
Customized Music On Hold Summary	Use this section of the screen to manage the music on hold profiles that you create.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This indicates the name of the music on hold profile.
Description	This displays the description associated with the music on hold profile.
Quota Usage	This bar displays what percentage of the ISG50’s audio file storage space is currently in use. When the storage space is almost full, you should consider deleting unused audio files before adding more.
Total	This is the ISG50’s total available audio recording time.
Used	This is how much of the ISG50’s audio recording time is already used.
Free	This is the ISG50’s remaining available audio recording time.
Delete Audio File	Click **Unused** to delete the audio recordings that not none of the ISG50’s features are set to use or **All** to delete all of the audio recordings.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

34.6.1 Add or Edit Custom Music On Hold

Use this screen to create or edit a music on hold profile and upload an audio file to it.

In the **Configuration > PBX > Call Service > Music On Hold** screen, click **Add** or **Edit** to open the screen as shown.

Figure 361 Add Customized Music on Hold



To upload a Music file, browse to the location of the file (.wav) and then click Upload.

No Audio File!

The following table describes the labels in this screen.

Table 196 Add Customized Music on Hold

LABEL	DESCRIPTION
Name	Enter a name for the music on hold profile.
Description	Enter a description for the music on hold profile.
Upload Music File	Click **Browse** to locate an audio file to be used as the auto-attendant greeting message, and **Upload** to copy it to IP-PBX. The audio files you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The total play time of all the music files combined must be less than 30 minutes.
Audio File State	This indicates whether an audio file has been uploaded to the ISG50 or not. You can also **Playback** the audio file to hear how it sounds.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

34.7 The Call Transfer Screen

Call Transfer allows you to transfer an incoming call (that you have answered) to another phone by doing the following.

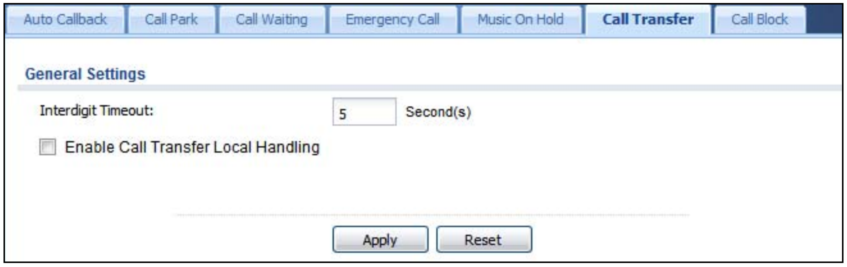
1 Dial a predefined feature code (for example, ***96** by default) followed by the number to which you want to transfer the call to operate the intercom. See more feature code information in Section 27.3 on page 433.

2 After you hear the ring signal or the second party answers it, hang up the phone.

34.7.1 Configuring the Call Transfer Screen

Use this screen to configure call transfer on the ISG50. Click **Configuration > PBX > Call Service > Call Transfer** to open the screen as following.

Figure 362 Configuration > PBX > Call Service > Call Transfer


Auto Callback
Call Park
Call Waiting
Emergency Call
Music On Hold
Call Transfer
Call Block
Apply
Reset

General Settings

Interdigit Timeout: 5 Second(s)

☐ Enable Call Transfer Local Handling

The following table describes the labels in this screen.

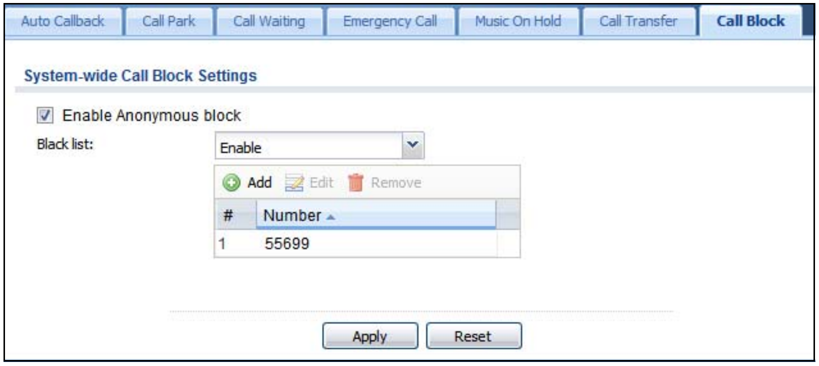
Table 197 Configuration > PBX > Call Service > Call Transfer

LABEL	DESCRIPTION
Interdigit timeout	Enter the maximum number of seconds (1-30) the ISG50 waits for each digit input of a complete callee number after you press the flash key on the phone. If the ISG50 cannot receive the next digit entered within this time period, the ISG50 processes digits you have dialed.
Enable Call Transfer Local Handling	Select this to allow a caller to transfer a current external call (via an outbound line group) to another extension. Otherwise, clear it to not allow this.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to set every field in this screen to its last-saved value.

34.8 The Call Block Screen

Use this screen to have the ISG50 not accept incoming calls from specific phone numbers or calls without caller ID. Click **Configuration > PBX > Call Service > Call Block** to view the screen as shown next.

Figure 363 Configuration > PBX > Call Service > Call Block


Auto Callback
Call Park
Call Waiting
Emergency Call
Music On Hold
Call Transfer
Call Block
Add
Edit
Remove
Apply
Reset

System-wide Call Block Settings

☑ Enable Anonymous block

Black list: Enable

#	Number
1	55699

Each field is described in the following table.

Table 198 Configuration > PBX > Call Service > Call Block

LABEL	DESCRIPTION
Enable Anonymous block	Select this to block calls without caller ID from being routed by the ISG50. Clear it to allow any incoming calls routed by the ISG50.
Black list	Select **Disable** to turn call blocking off on the ISG50. Select **Enable** to turn on call blocking on the ISG50. When you select **Enable**, use the table that displays to set up a list of phone numbers that are not allowed to call into the ISG50.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Number	This is a telephone number the ISG50 blocks from calling extensions in your telephone network. When adding or editing an entry, type the telephone number. You can also use the letters **X**, **Z** and **N** to represent numbers you want to block. The letter "**X**" represents any digit from 0-9, **Z** any digit from 1-9 and **N** any digit from 2-9. For example, enter **023XXXXXX** to block any 9 digit number that starts with **023** from calling the extensions configured on the ISG50. Furthermore, you can use the period (**.**) as a wildcard, to block any numbers that begin with a pattern of digits you specify. For example, enter **555.** to block any numbers starting with the string **555** from calling the extensions configured on the ISG50.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

35

Call Recording

35.1 Overview

Use the call recording feature to record all the calls going to or from specific extensions or trunks or let users record calls. This is useful if you need to monitor certain individuals' calls. It is also useful for conference call recording, the administrator may configure the ISG50 to record a Meetme conference room and use the recording as the meeting minutes. The ISG50 supports full-time and on-demand recording.

- Full-time recording records all calls to or from the trunks and peers you specify.
- On-demand recording allows users of internal extensions to dial a number to have the ISG50 record the current call on whichever extension he is using.

Note: Call recording requires a valid subscription to use. See Chapter 11 on page 229 for details.

35.1.1 What You Can Do in this Chapter

- Use the **Call Recording** screen to configure call recording on the ISG50. See Section 35.2 on page 545.

35.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Supported Extension Types:

- SIP
- FXS
- Meetme

Supported Trunk Types:

- FXO
- BRI
- SIP trunk
- Trusted Peer

Other Important Call Recording Details

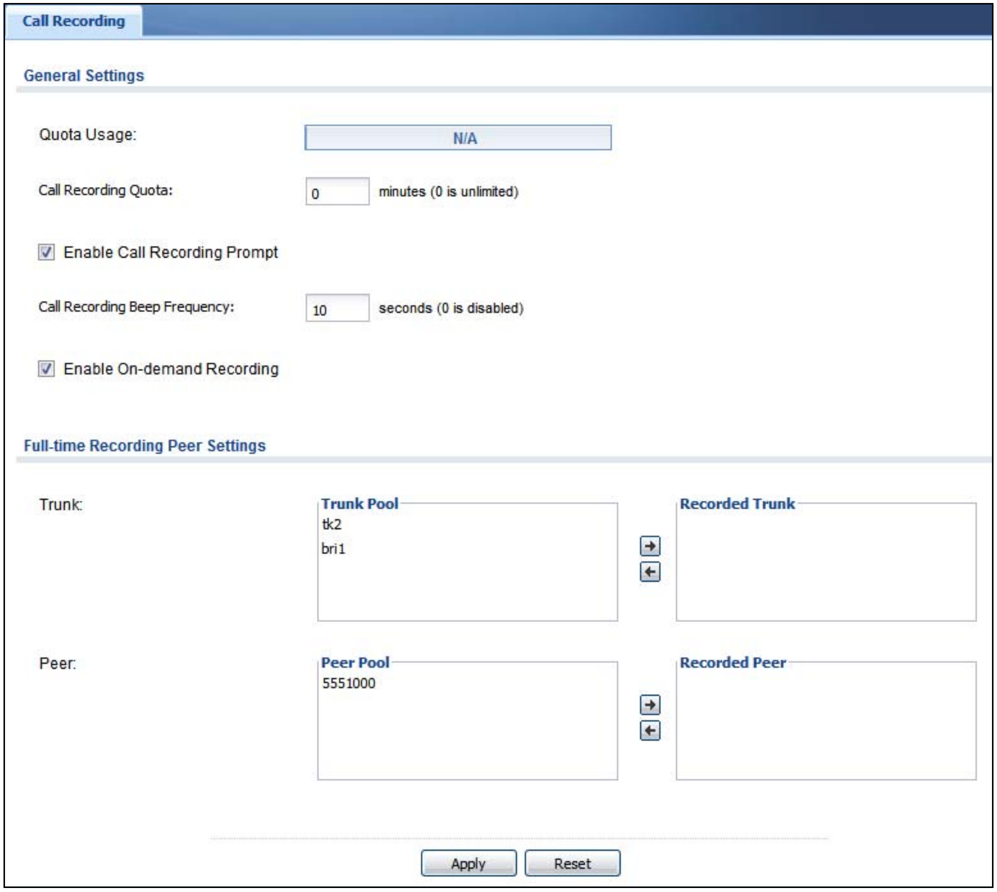
- You must connect a USB storage device (not included) for the ISG50 to use to store call recordings.

- The maximum call recording time depends on the storage capacity of the connected USB storage device.
- Once the ISG50 is recording the maximum number of channels defined by the call recording license, it does not record additional concurrent calls. See Chapter 11 on page 229.
- The ISG50 generates a warning log when the remaining call recording time goes below five days and an alert if it goes below 24 hours. The ISG50 stops recording calls once the hard drive is full.
- Calls recordings are saved in .wav format files.

35.2 Configuring the Call Recording Screen

Use this screen to configure call recording on the ISG50. Click **Configuration > PBX > Call Recording** to open the screen as following.

Figure 364 Configuration > PBX > Call Recording



Call Recording
General Settings
Full-time Recording Peer Settings
Trunk Pool
Recorded Trunk
Peer Pool
Recorded Peer
Apply
Reset

Quota Usage: N/A

Call Recording Quota: 0 minutes (0 is unlimited)

☑ Enable Call Recording Prompt

Call Recording Beep Frequency: 10 seconds (0 is disabled)

☑ Enable On-demand Recording

Trunk: Trunk Pool: tk2, bri1

Peer: Peer Pool: 5551000

The following table describes the labels in this screen.

Table 199 Configuration > PBX > Call Recording

LABEL	DESCRIPTION
Quota Usage	This bar displays what percentage of the ISG50's call recording storage space is currently in use. When the storage space is almost full, you should consider deleting call recording files before adding more.
Call Recording Quota	Set the maximum number of minutes of call recording on the ISG50.
Enable Call Recording Prompt	Select this to have the ISG50 play a recording notification message at the beginning of calls that it records.
Call Recording Beep Frequency	The ISG50 plays a beep at a regular interval to remind the call participants about the recording. Set the interval here. 0 means there is no beep.
Enable On-demand Recording	Select this to allow any user of an internal extension to dial a number to have the ISG50 record his current call on whichever extension he is using. See Section 27.3 on page 433 to set the number a user dials to enable on-demand call recording.
Full-time Recording Peer Settings	Use this list boxes to select the trunks the ISG50 records all the time.
Trunk	Use this section to specify for which trunks the ISG50 should record all outgoing and incoming calls. Select a trunk in the **Trunk Pool** column and click the right arrow to select it for recording. Select a trunk in the **Recorded Trunk** column and click the left arrow to not record this trunk's calls.
Peer	Use this section to specify for which extensions the ISG50 should record all outgoing and incoming calls. Select an extension in the **Peer Pool** column and click the right arrow to select it for recording. Select an extension in the **Recorded Peer** column and click the left arrow to not record this extension's calls.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

36

Meet-me Conference

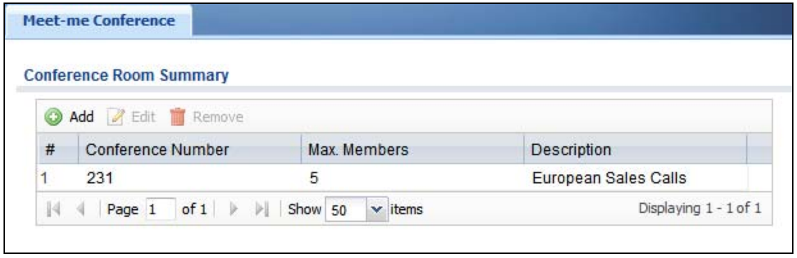
The ISG50 allows you to set up specific extension numbers which callers can dial to join a conference call. This type of extension is referred to as a conference room number. You can restrict the number of callers that can join the conference call. You can also specify a PIN (Personal Identification Number) for the conference room. Callers must enter the PIN before they can enter the conference room.

Callers within your organization simply call the conference room number to join the conference call. Callers from the outside dial the conference room number after they are prompted by auto-attendant to dial the extension they wish to call.

36.0.1 Configuring the Meet-me Conference Screen

Use this screen to manage conference call rooms on the ISG50. Click **Configuration > PBX > Meet-me Conference** to view the following screen.

Figure 365 Configuration > PBX > Meet-me Conference



#	Conference Number	Max. Members	Description
1	231	5	European Sales Calls

The following table describes the labels in this screen.

Table 200 Configuration > PBX > Meet-me Conference

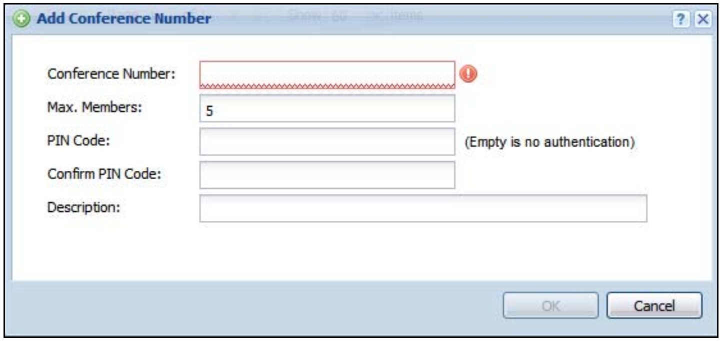
LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Conference Number	This field displays the conference room number. This is the extension callers should dial to enter this conference room.
Max. Members	This is the number of participants that can join this conference call at any one time.
Description	This field displays the description you enter to identify this conference room.

36.0.2 The Meet-me Conference Calling Edit and Add Screen

Use this screen to configure a new conference room. Click the **Add** icon to see the screen as shown.

Note: The screen for editing an existing conference room has the same fields as the screen shown below. You can access the **Conference Room Edit** screen by clicking the **Edit** icon in the **Conference Room List** screen.

Figure 366 Conference Room Add



Max. Members: 5

The following table describes the labels in this screen.

Table 201 Conference Room Add

LABEL	DESCRIPTION
Conference Number	Enter the extension (3 to 10 digits in length) callers should dial to enter this conference room. If you are editing an existing conference room entry, this field is read-only.
Max. Members	Specify the maximum number of participants for this conference room. Once the maximum number of participants join this conference call, the conference room will be closed until an existing participant leaves the conference room.
PIN Code	Type the numeric password callers need to enter to join a conference room. If this field is left blank, then callers can enter this conference room without entering a PIN.
Confirm PIN Code	Retype the PIN.
Description	Enter a brief description to identify this conference room.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

37

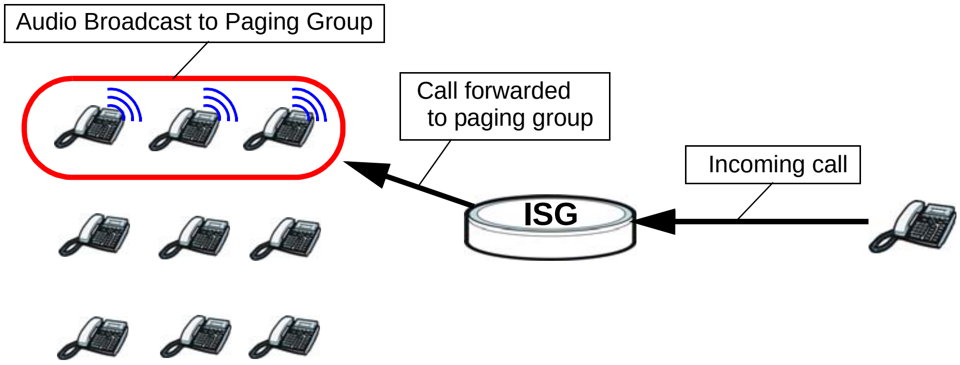
Paging Group

37.1 Overview

This chapter shows you how to create and manage paging groups on the ISG50. Paging groups are sets of extensions through which a caller can make a one-way announcement by dialing a single number. It works much like a public address system. A caller wanting to make an announcement dials a pre-configured number representing a group of extensions. The telephones for the group's extensions all automatically pick up at the same time and play what the caller says. The paged extensions cannot reply to the caller nor talk to each other.

Note: The IP phones must support a compatible auto pickup function for the paging groups feature to work.

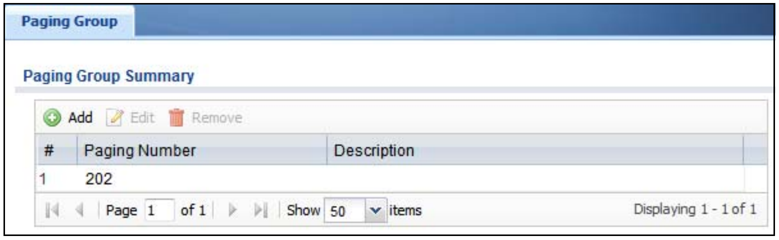
Figure 367 Paging Group Overview


Audio Broadcast to Paging Group
Call forwarded to paging group
Incoming call
ISG

37.2 The Paging Group Screen

Use this screen to manage paging groups on the ISG50. To access this screen, click **Configuration > PBX > Paging Group**.

Figure 368 Configuration > PBX > Paging Group


Paging Group
Add
Edit
Remove
Page 1 of 1
Show 50 items

Paging Group Summary

#	Paging Number	Description
1	202	

Displaying 1 - 1 of 1

Each field is described in the following table.

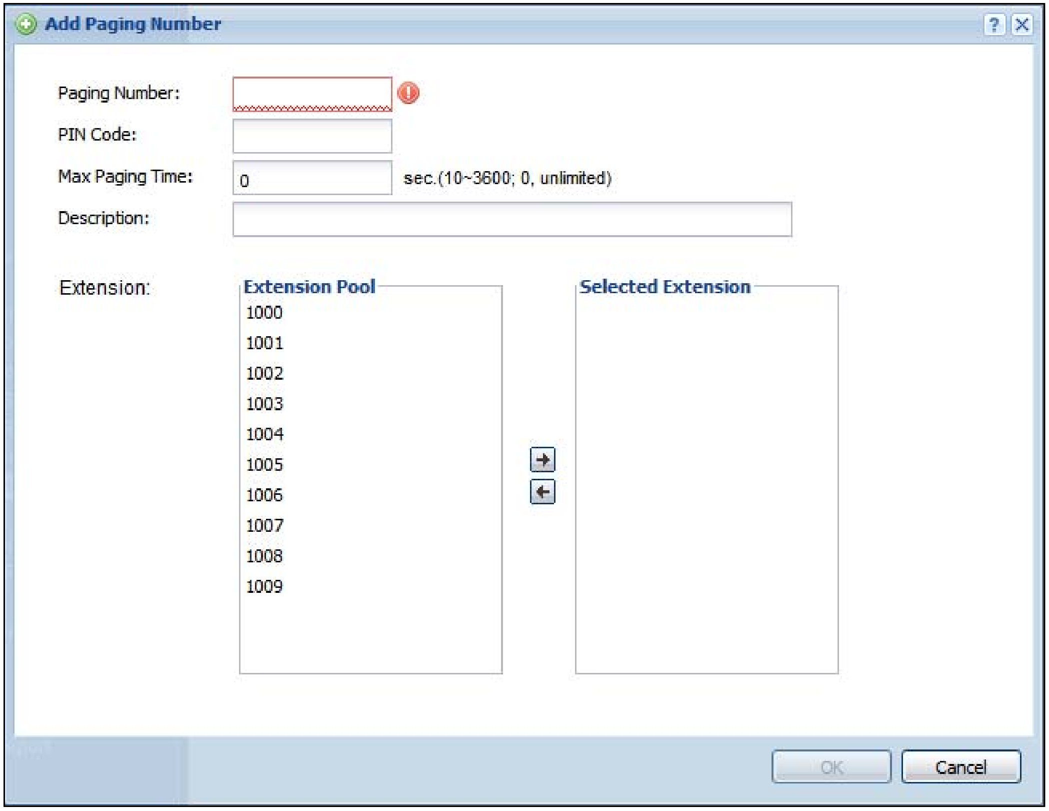
Table 202 Configuration > PBX > Paging Group

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Paging Number	This field displays the number you have to dial to broadcast through the extensions in this page group.
Description	This field displays the description of the paging group.

37.2.1 The Add/Edit Paging Group Screen

The screens for editing or adding page groups on the ISG50 contain the same fields. Only the screen used to add page groups is shown below. Click the **Add** (or **Edit**) icon in the **Paging Group** configuration screen to view the screen as shown.

Figure 369 Add Paging Group


Add Paging Number
Paging Number:
PIN Code:
Max Paging Time:
sec.(10~3600; 0, unlimited)
Description:
Extension:
Extension Pool
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
Selected Extension
OK
Cancel

Max Paging Time: 0

Each field is described in the following table.

Table 203 Add Paging Group

LABEL	DESCRIPTION
Paging Number	Type the number you have to dial to call the extensions in this page group. This number can be from 3 to 10 digits long.
PIN Code	Type the password you have to dial to call the extensions in this page group. This number can be 3-10 digits long. If you leave this field blank then callers do not have to dial a PIN code to call the extensions in this page group.
Max Paging Time	Type the maximum number of seconds that a person can page a group of extensions. Use 0 to set the paging time to “unlimited”.
Description	Type a description for this page group.
Extensions	Move the extensions you want to be in this page group to the **Selected Extensions** column by highlighting them in the **Extension Pool** column and clicking the **Right** button. Remove the extensions you don’t want to be in this page group from the **Selected Extensions** column by highlighting them and clicking the **Left** button.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38

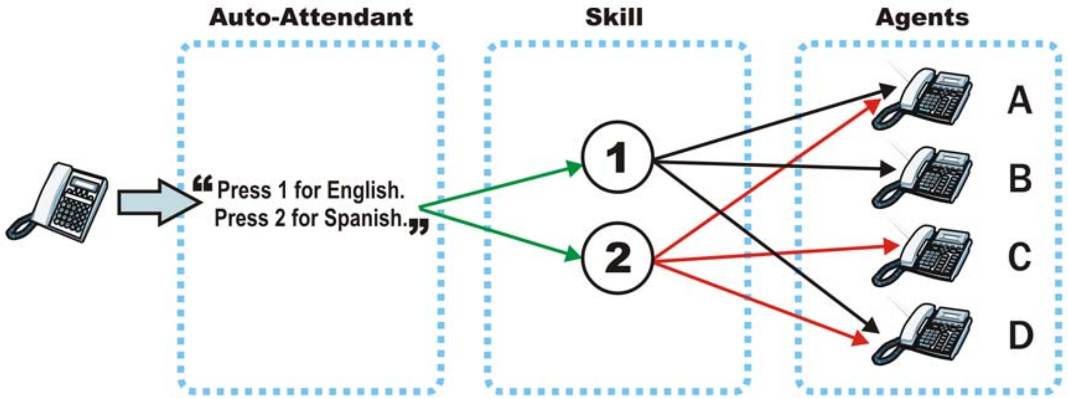
ACD

38.1 Overview

This chapter shows you how to configure Automatic Call Distribution (ACD). ACD utilizes Skill-Based Routing (SBR), which allows you to distribute incoming calls to specific groups of phones based on assigned skills.

When the ISG50 receives an incoming call, the auto-attendant presents the caller with a list of available skills and the key codes to access them. Each skill is linked to a specific group of agents. One agent from the group can be selected to answer the incoming call based the rules defined by the associated skill.

Figure 370 ACD Example



For example, a call comes in and the ISG50 prompts the caller with an auto-attendant greeting, asking him to choose which "skill" he requires: an English-speaking (**1**) or Spanish-speaking (**2**) representative. In this case, the auto-attendant's message may say something to the effect of "Thank you for calling Acme Mail Order Company. Press 1 for English service, o selecciones el número 2 para Español." Once the caller makes his selection, the call is routed to an agent according to the skill rule set. If the caller presses the 1 key for English then, the ISG50 routes the call to 1 of 3 available agents (**A**, **B**, and **D**) whose IDs appear in the English skill's associated agent list and based upon their current availability.

38.1.1 What You Can Do in this Chapter

- Use the **ACD Global** screen to set the global "wrap up" time for each extension in the ACD system. See Section 38.2 on page 556.
- Use the **Agent** screen to manage the ACD agent identities. See Section 38.3 on page 556.
- Use the **Skill** screen to manage the ACD skills. See Section 38.4 on page 558.
- Use the **Hunt Group** screen to manage the hunt groups. See Section 38.5 on page 562.

- Use the **Skill Menu** screen to create menus that a caller can use while in the queue waiting for an agent to respond. See Section 38.6 on page 564.

38.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Agent

An agent is a member of an Automated Call Distribution system who receives incoming calls. Agents are usually classified according to “skills”. For example, a customer support representative in an automotive parts company may be classified as a member of the “Brakes and Tires” skill. As such, the ISG50 auto attendant would only route calls to him related to those two topics.

Agent Feature Code

The agent-specific feature code is: *****03**. This allows an agent to get a login prompt and log into the ISG50 to notify the device that his extension is a member of the Automated Call Distribution system. This code is also used to log out.

When logged in as an agent, you can put your phone on “pause” status so it temporarily cannot receive incoming calls from the ISG50. To do so, type: *****04**. Type it a second time to un-pause your phone.

Note: This feature code cannot be modified. For more information on feature codes and how to use them, see Section 27.3 on page 433.

Skill

In the context of ACD, a skill is a set of rules that bridge the auto-attendant on one side and the agents on the other. The rules tell the ISG50 exactly how to route calls to specific agents based on the input it receives from the caller interacting with the auto-attendant.

Hunt Group

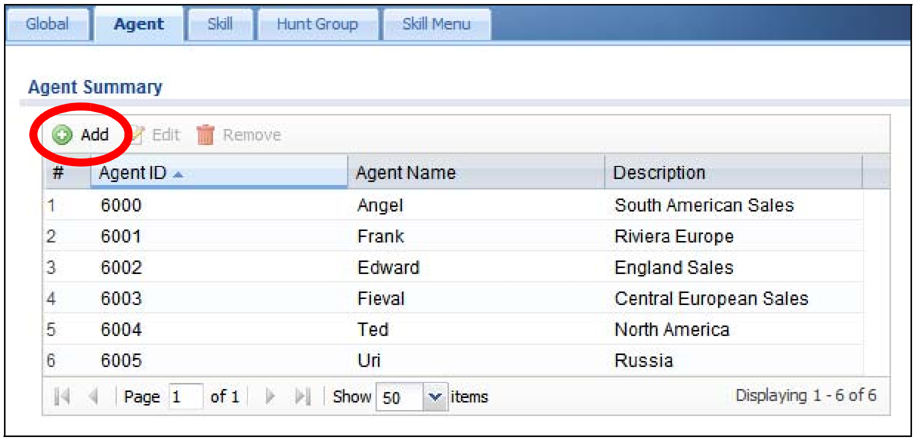
Allows a caller to simply dial a number to reach a group of extensions. The extensions ring based on a ringing method you configure. For example, all extensions can ring at the same time until the call is picked up or extensions in the group ring in a random order until the call is picked up.

Auto Attendant

The ISG50’s auto attendant feature is an integral part of the ACD system. When a caller first dials in, the auto-attendant receives the call. The auto attendant then passes the call to the ACD system. See Chapter 30 on page 477 for how to configure auto attendants.

To link the ACD system with the auto-attendant feature:

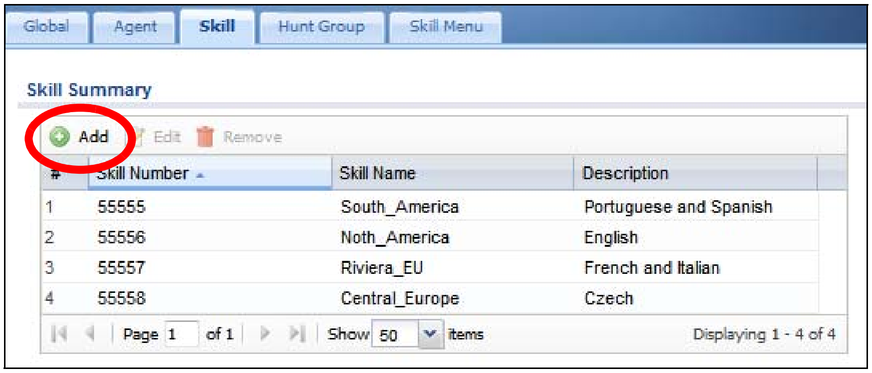
1 Create at least 2 agent identities in the ACD system (Section 38.3 on page 556) to ultimately receive incoming calls after they have been routed by the ISG50. You can click **Configuration > PBX > ACD > Agent** to open this screen.


Global
Agent
Skill
Hunt Group
Skill Menu
Agent Summary
Add
Edit
Remove

#	Agent ID	Agent Name	Description
1	6000	Angel	South American Sales
2	6001	Frank	Riviera Europe
3	6002	Edward	England Sales
4	6003	Fieval	Central European Sales
5	6004	Ted	North America
6	6005	Uri	Russia

Page 1 of 1 Show 50 items
Displaying 1 - 6 of 6

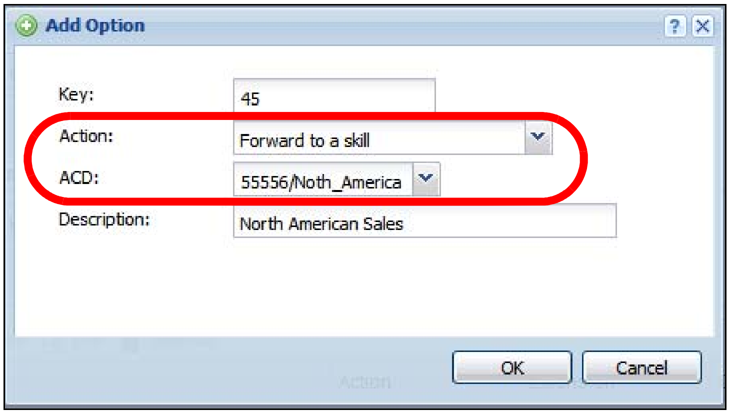
2 Define at least 1 skill in the ACD system (Section 38.4 on page 558). The rules defined here will help the ISG50 properly route calls to the agent identities created in step 1. You can click **Configuration > PBX > ACD > Skill** to open this screen.


Global
Agent
Skill
Hunt Group
Skill Menu
Skill Summary
Add
Edit
Remove

#	Skill Number	Skill Name	Description
1	55555	South_America	Portuguese and Spanish
2	55556	Noth_America	English
3	55557	Riviera_EU	French and Italian
4	55558	Central_Europe	Czech

Page 1 of 1 Show 50 items
Displaying 1 - 4 of 4

3 Finally, link the skill with your auto-attendant by forwarding calls from it to the skill you created in step 2 (Section 31.3.2 on page 509). You can click the **Add** or **Edit** icon in the **Configuration** > **PBX** > **Outbound Line Management** > **Auto-Attendant > Customized** screen and then click the **Office Hour** tab to open this screen.


Add Option

Key: 45
Action: Forward to a skill
ACD: 55556/Noth_America
Description: North American Sales

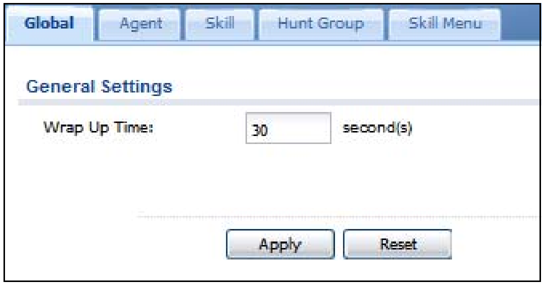
OK
Cancel

38.2 The ACD Global Screen

Use this screen to set the global “wrap up” time for each extension in the ACD system. This is how long the ISG50 waits before sending new calls to the agent.

Click **Configuration > PBX > ACD > ACD Global** to open this screen.

Figure 371 ACD > ACD Global Setting


Global
Agent
Skill
Hunt Group
Skill Menu
General Settings
Apply
Reset

Wrap Up Time: 30 second(s)

Each field is described in the following table.

Table 204 ACD > ACD Global Setting

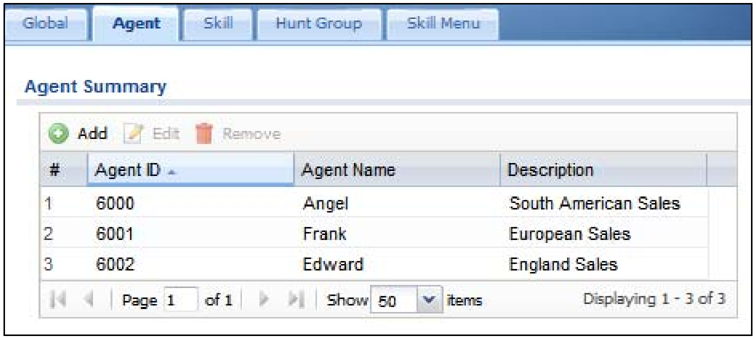
LABEL	DESCRIPTION
Wrap Up Time	Enter a number of seconds here that the ISG50 waits before re-queuing the agent to receive new incoming calls. You can enter a number between 1 and 86400.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

38.3 The Agent Screen

This screen allows you to manage the ISG50’s agent identities. It can also serve as a jumping off point for creating new ones or editing ones previously created.

Click **Configuration > PBX > ACD > Agent** to open this screen.

Figure 372 ACD > Agent List


Global
Agent
Skill
Hunt Group
Skill Menu
Agent Summary
Add
Edit
Remove
Page 1 of 1
Show 50 items
Displaying 1 - 3 of 3

#	Agent ID	Agent Name	Description
1	6000	Angel	South American Sales
2	6001	Frank	European Sales
3	6002	Edward	England Sales

Each field is described in the following table.

Table 205 ACD > Agent List

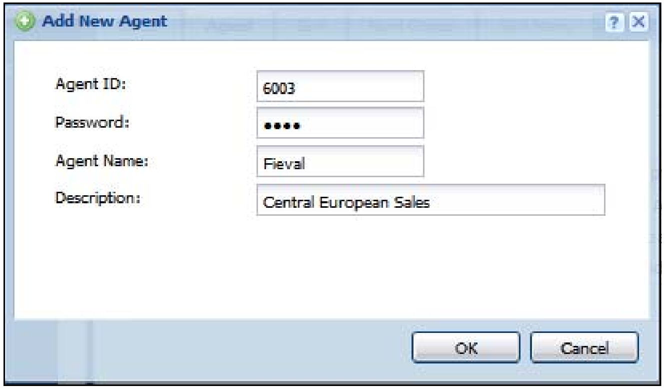
LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Agent ID	This indicates the identification number of the agent.
Agent Name	This indicates the name of the agent.
Description	This displays a brief description about the agent.

38.3.1 The Agent Settings Screen

Use this screen to create or edit an agent's settings.

Click either the **Add** or **Edit** icons in the **Agent List** screen to display the options as shown next.

Figure 373 Agent List > Agent Setting



Agent ID: 6003
Password: ●●●●
Agent Name: Fieval
Description: Central European Sales

Each field is described in the following table.

Table 206 Agent List > Agent Setting

LABEL	DESCRIPTION
Agent ID	Enter an identification number for this agent. It can be 3~20 digits (0-9). No spaces, underscores, or hyphens are allowed. This number cannot overlap with existing extension numbers. An agent must use this ID to log into the ACD system. Note: To get a login prompt, enter the feature code *****03** on your phone's keypad. You can also use this code to log out later.
Password	Enter a password for this agent. It can be any combination of 1~32 digits (0-9). No spaces, underscores, or hyphens are allowed. An agent must use this password to log into the ACD system. Note: To get a login prompt, enter the feature code *****03** on your phone's keypad. You can also use this code to log out later.

Table 206 Agent List > Agent Setting (continued)

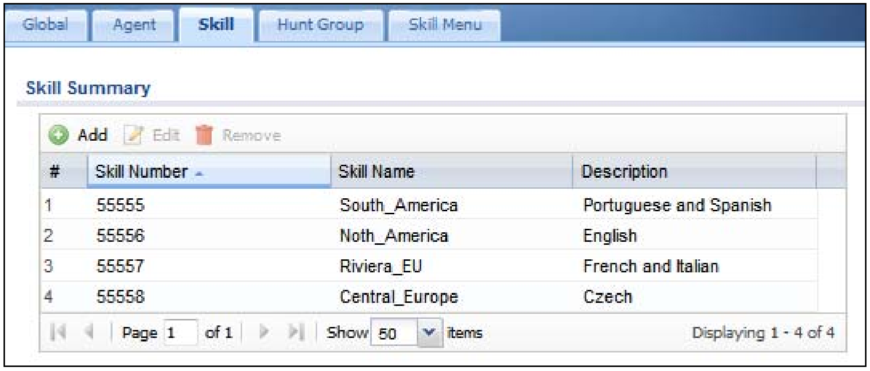
LABEL	DESCRIPTION
Agent Name	Enter the name of the agent associated with this ID. It can be any combination of 1~32 alphanumeric characters (a-z, A-Z, 0-9). No asterisks (*) or exclamation points (!) allowed.
Description	Enter a description for this agent ID. It can be any combination of 0~64 alphanumeric characters (a-z, A-Z, 0-9). No asterisks (*) or exclamation points (!) allowed.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.4 The Skill Screen

This screen allows you to manage the ACD skills. It can also serve as a jumping off point for creating new ones or editing ones previously created.

Click **Configuration > PBX > ACD > Skill** to open this screen.

Figure 374 ACD > Skill List



#	Skill Number	Skill Name	Description
1	55555	South_America	Portuguese and Spanish
2	55556	Noth_America	English
3	55557	Riviera_EU	French and Italian
4	55558	Central_Europe	Czech

Each field is described in the following table.

Table 207 ACD > Skill List

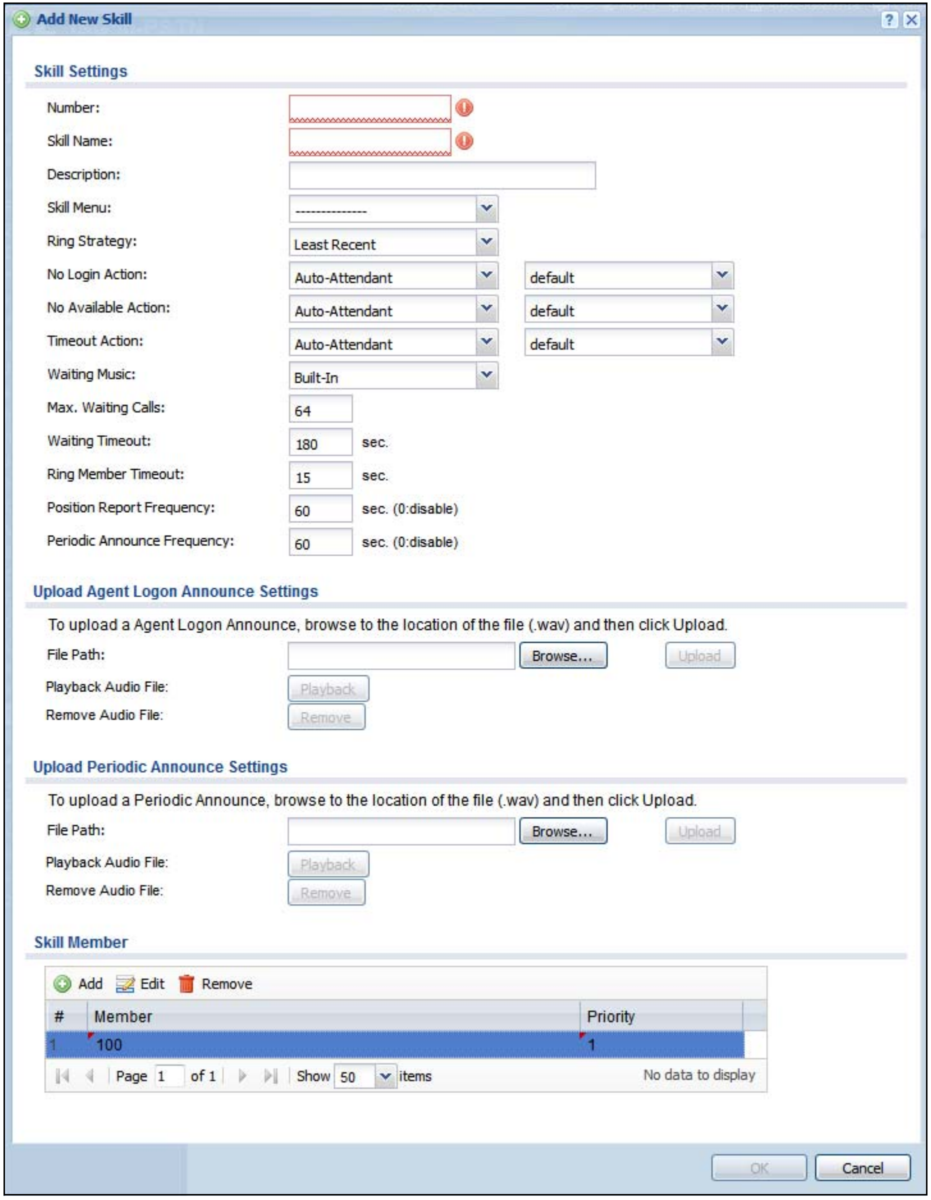
LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Skill Number	This indicates the phone number dialed to reach the agents associated with this particular skill.
Skill Name	This indicates the name of the skill.
Description	This displays the description associated with this skill.

38.4.1 The Add/Edit Skill Screen

Use this screen to create or edit a skill. A skill allows you to create rules for routing calls to a specific group of agents. You can also manage how calls to those agents are handled in the event that one or more of them is not logged on, or engaged in a conversation, and so on. Skills work in tandem with the auto-attendant. When a call comes in, the auto-attendant presents an automated menu system that guides the caller to a specific skill and from there to an agent.

Click **Add** or **Edit** in the **Skill** screen to display this screen.

Figure 375 Add Skill



Add New Skill

Skill Settings

Number:

Skill Name:

Description:

Skill Menu: --------------

Ring Strategy: Least Recent

No Login Action: Auto-Attendant default

No Available Action: Auto-Attendant default

Timeout Action: Auto-Attendant default

Waiting Music: Built-In

Max. Waiting Calls: 64

Waiting Timeout: 180 sec.

Ring Member Timeout: 15 sec.

Position Report Frequency: 60 sec. (0:disable)

Periodic Announce Frequency: 60 sec. (0:disable)

Upload Agent Logon Announce Settings

To upload a Agent Logon Announce, browse to the location of the file (.wav) and then click Upload.

File Path:

Playback Audio File:

Remove Audio File:

Upload Periodic Announce Settings

To upload a Periodic Announce, browse to the location of the file (.wav) and then click Upload.

File Path:

Playback Audio File:

Remove Audio File:

Skill Member

#	Member	Priority
1	100	1

Page 1 of 1 Show 50 items No data to display

Each field is described in the following table.

Table 208 Add Skill

LABEL	DESCRIPTION
Skill Setting	
Number	Enter the number to be dialed that uses this skill. It can be any combination of 3~10 digits (0-9). No spaces, underscores, or hyphens are allowed. When this screen is in **Edit** mode, this number cannot be changed.
Skill Name	Enter a name for this skill. It can be any combination of 1~32 alphanumeric characters (a-z, A-Z, 0-9). No asterisks (*) or exclamation points (!) allowed.
Description	Enter a description for this skill. It can be any combination of 0~64 alphanumeric characters (a-z, A-Z, 0-9). No asterisks (*) or exclamation points (!) allowed.
Skill Menu	Associate this skill with a skill menu. For more on skill menus, see Section 38.6 on page 564.
Ring Strategy	Select the method for the ISG50 to decide the ring order of extensions associated with this skill. • **Least Recent** - This action rings the agent associated with this skill who was least recently called. • **Round Robin** - This strategy takes turns ringing each available agent associated with this skill. • **Fewest Calls** - This strategy rings the agents who have received the fewest number of calls, in order, from lowest to highest. • **Random** - This strategy rings a random extension. • **Ring All** - This strategy rings all extensions at the same time until one answers.
No Login Action No Available Action Timeout Action	Fields: • **No Logon Action** - If all agents associated with a skill do not log in or log off, then this item defines how the ISG50 responds when calls are sent to them. • **No Available Action** - If no agent associated with this skill is available to take a call, then this item defines how the ISG50 responds when calls are sent to that agent. • **Timeout Action** - If a call to an agent associated with this skill times out, then this item defines how the ISG50 responds when calls are sent to that agent. Possible actions are: • **Join** - This action puts the call back in the queue for other extensions within this skill. (No Available Action only.) • **No Timeout** - This action keeps the caller on the line indefinitely while the extension is rung. (Timeout Action only.) • **Hang Up** - This action disconnects the call. • **Backup Skill** - This action sends the call to the next skill if one is associated with this one. When you select this option and you have already configured more than 1 skill, a submenu with all available skill appears. • **Page Group** - This action forwards the call to the page group you specify. See Chapter 37 on page 549 for details on this feature. • **Hunt Group** - This action forwards the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Auto Attendant** - This action routes the call back to the auto attendant system you specify. • **Extension** - This action routes the call to the specified extension. • **Voice Mail** - This action engages the extension owner’s voice mail.
Waiting Music	Play music or the ring tone while a caller waits for an agent to pick up. For more on Music On Hold, see Section 34.6 on page 539.
Max. Waiting Calls	Enter the maximum number of calls (up to 999) to be put on hold while calling the agents associated with this skill.

Table 208 Add Skill (continued)

LABEL	DESCRIPTION
Waiting Timeout	Enter the duration in seconds (up to 99999) that the call to the agents associated with the skill rings before timing out. Once a call times out, the action defined in **Timeout Action** applies. This timeout only applies to calls in the queue that have not yet been routed to a particular agent.
Ring Member Timeout	Enter the duration in seconds (up to 99999) that a call to a specific agent associated with this skill rings before timing out. Once a call times out, it is routed to a different agent.
Position Report Frequency	Enter the duration in seconds (up to 99999) that the ISG50 waits before informing the caller on hold what their current position in the queue is. This report occurs periodically and continues until either the caller hangs up or the agent answers. For example, if a caller is second in the queue then the ISG50 may say, “You are currently call number 2” every 60 seconds. If you enter a “0” for this field, the option is disabled.
Periodic Announce Frequency	Enter the duration in seconds (up to 99999) that the ISG50 waits before playing a previously uploaded audio file. This announcement occurs periodically and continues until either the caller hangs up or the agent answers. For example, a caller to the Acme Mail Order Company may hear, “Thank you for calling us. A service representative will be with you momentarily” every 240 seconds. If you enter a “0” for this field, the option is disabled.
Agent Logon Announce Settings Upload Periodic Announce Settings	Fields: • Announce - The ISG50 plays this file first when the agent answers the phone, then it connect his phone to the call. It can be used to announce which skill the incoming caller requires, which is especially useful when one agent is associated with multiple skills. For example, if an agent is associated with the skills “English” and “Spanish”, then the announce audio file played before receiving a call sent to him by way of the English skill may say “This caller speaks English.” • Periodic Announce - The ISG50 plays this file to a caller on hold every X number of seconds and can be used to keep the caller apprised of their status. For example, a caller may hear the following every 30 seconds: “Thank you for your patience. Please continue holding.” Possible actions are: • Click the **Browse** button to find an audio file on your computer that you want to upload. • Click the **Upload** button to upload the selected file to the ISG50. • Click the **Playback** button to listen to the audio file once it has been uploaded. • Click the **Remove** button to delete an uploaded audio file. The audio files you upload must meet the following criteria: • PCM format, 16 kHz, 16-bit, mono mode (*.wav). • The play time of each audio file must be less than 30 seconds.
Skill Member	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.

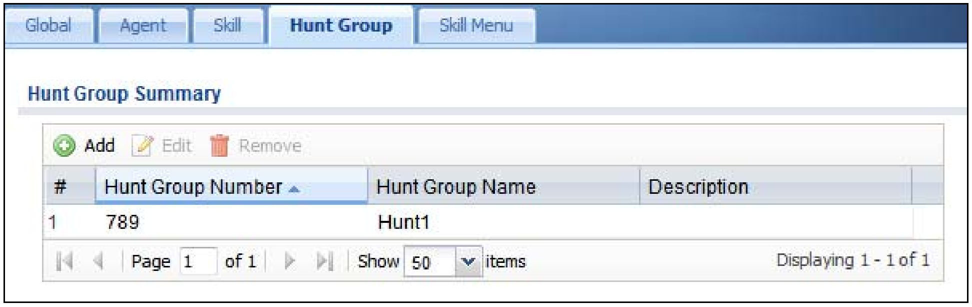
Table 208 Add Skill (continued)

LABEL	DESCRIPTION
Member	This list indicates all members who are assigned to this skill. When adding or editing an entry select the member from the drop-down list.
Priority	The priority indicates to which agent incoming calls are routed first. When adding or editing an entry type the priority (1 highest to 5 lowest). If multiple agents share the same priority, then the **Ring Strategy** applies first to the highest priority group, then if all those agents are engaged it applies to the next group, and so on.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.5 The Hunt Group Screen

Use this screen to manage hunt groups on the ISG50. To access this screen, click **Configuration > PBX > ACD > Hunt Group**.

Figure 376 Configuration > PBX > ACD > Hunt Group



#	Hunt Group Number	Hunt Group Name	Description
1	789	Hunt1	

Each field is described in the following table.

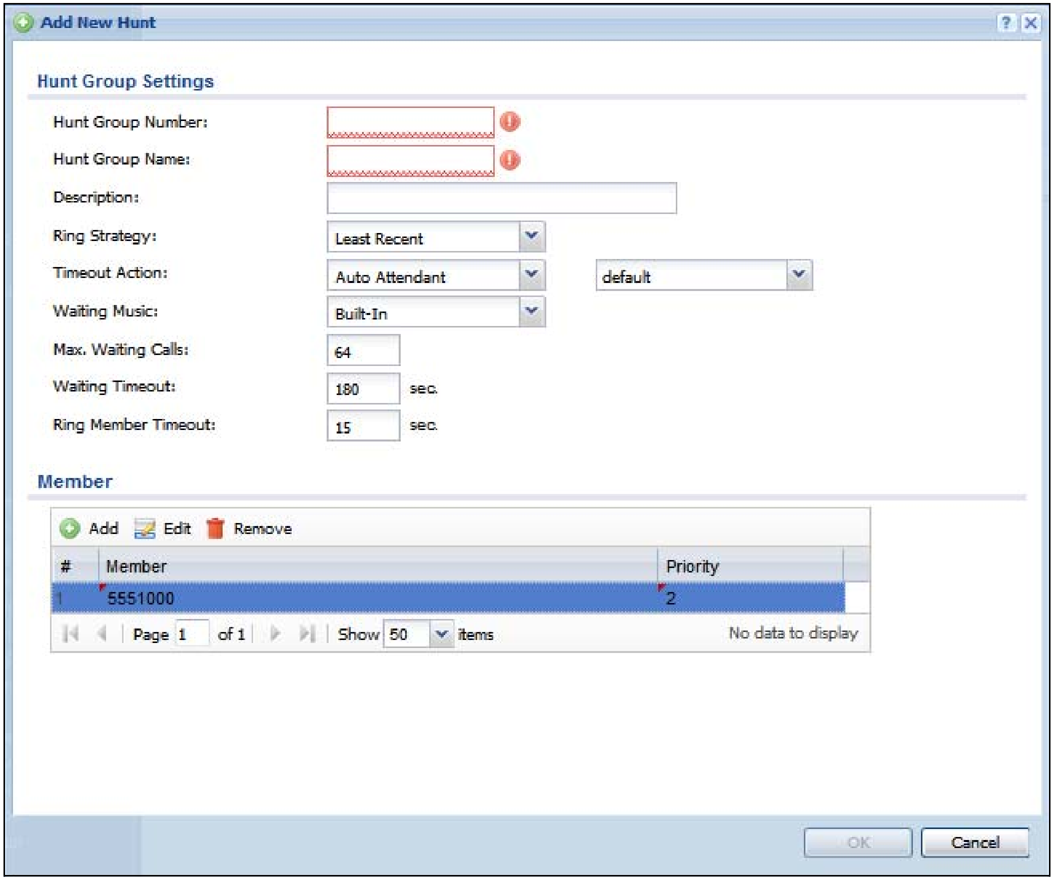
Table 209 Configuration > PBX > ACD > Hunt Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Hunt Group Number	This field displays the number you have to dial to call the extensions in this hunt group.
Hunt Group Name	This field displays the name of the hunt group.
Description	This field displays the description of the hunt group.

38.5.1 The Add/Edit Hunt Group Screen

The screens for editing or adding Hunt groups on the ISG50 contain the same fields. Click the **Add** (or **Edit**) icon in the **Hunt Group** configuration screen to view the screen as shown.

Figure 377 Add Hunt Group



Hunt Group Number:
Hunt Group Name:
Description:
Ring Strategy: Least Recent
Timeout Action: Auto Attendant default
Waiting Music: Built-In
Max. Waiting Calls: 64
Waiting Timeout: 180 sec.
Ring Member Timeout: 15 sec.

#	Member	Priority
1	5551000	2

Page 1 of 1 Show 50 items No data to display

Each field is described in the following table.

Table 210 Add Hunt Group

LABEL	DESCRIPTION
Hunt Group Number	Type the number you have to dial to call the extensions in this hunt group.
Hunt Group Name	Enter a name for this hunt group.
Description	Type a description for this hunt group.
Ring Strategy	Select the method for the ISG50 to decide the ring order of the hunt groups extensions. • **Least Recent** - This action rings the agent associated with this skill who was least recently called. • **Round Robin** - This strategy takes turns ringing each available agent associated with this skill. • **Fewest Calls** - This strategy rings the agents who have received the fewest number of calls, in order, from lowest to highest. • **Random** - This strategy rings a random extension. • **Ring All** - This strategy rings all extensions at the same time until one answers.

Table 210 Add Hunt Group (continued)

LABEL	DESCRIPTION
Timeout Action	If a call to an extension of the hunt group times out, then this item defines how the ISG50 responds when calls are sent to that member. Possible actions are: • **No Timeout** - This action keeps the caller on the line indefinitely while the extension is rung. (Timeout Action only.) • **Hang Up** - This action disconnects the call. • **Backup Skill** - This action sends the call to the next skill if one is associated with this one. When you select this option and you have already configured more than 1 skill, a submenu with all available skill appears. • **Hunt Group** - This action forwards the call to the hunt group you specify. See Section 38.5 on page 562 for details on this feature. • **Auto Attendant** - This action routes the call back to the auto attendant system that first greeted the caller. • **Extension** - This action routes the call to the specified extension. • **Voice Mail** - This action engages the extension owner's voice mail.
Waiting Music	Play music or the ring tone while a caller waits for one of the hunt group's extensions to pick up. For more on Music On Hold, see Section 34.6 on page 539.
Max. Waiting Calls	Enter the maximum number of calls (up to 999) to be put on hold while calling this hunt group's extensions.
Waiting Timeout	Enter the duration in seconds (up to 99999) that the call to the hunt group's extensions rings before timing out. Once a call times out, the action defined in **Timeout Action** applies. This timeout only applies to calls in the queue that have not yet been routed.
Ring Member Timeout	Enter the duration in seconds (up to 99999) that a call to a specific member extension of this hunt group rings before timing out. Once a call times out, it is routed to a different extension.
Member	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Member	This list indicates all extensions that are members of this hunt group. When adding or editing an entry select the member from the drop-down list.
Priority	The priority indicates to which extension incoming calls are routed first. When adding or editing an entry type the priority (1 highest to 5 lowest). If multiple extensions share the same priority, then the **Ring Strategy** applies first to the highest priority group, then if all those extensions are engaged it applies to the next group, and so on.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.6 The Skill Menu Screen

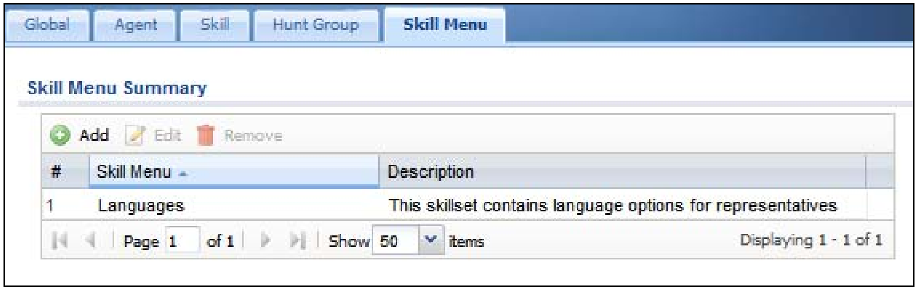
This screen allows you to create menus that a caller can use while in the queue waiting for an agent to respond. Skill menus are self-contained auto-attendants limited to the ACD system.

For example, if a caller enters the queue for the “English” skill but an English-speaking sales representative hasn’t yet picked up, he will periodically hear “Press 0 to exit. Press 3 for a Spanish-speaking representative. Press 4 for a French-speaking representative. Press 5 for a Russian-speaking representative.”

The **Periodic Announce** settings for a skill menu can be configured in the **Skill Settings** screen. See Section 38.4.1 on page 559 for more details.

Click **Configuration > PBX > ACD > Skill Menu** to open this screen.

Figure 378 ACD > Skill Menu



#	Skill Menu	Description
1	Languages	This skillset contains language options for representatives

Each field is described in the following table.

Table 211 ACD > Skill Menu

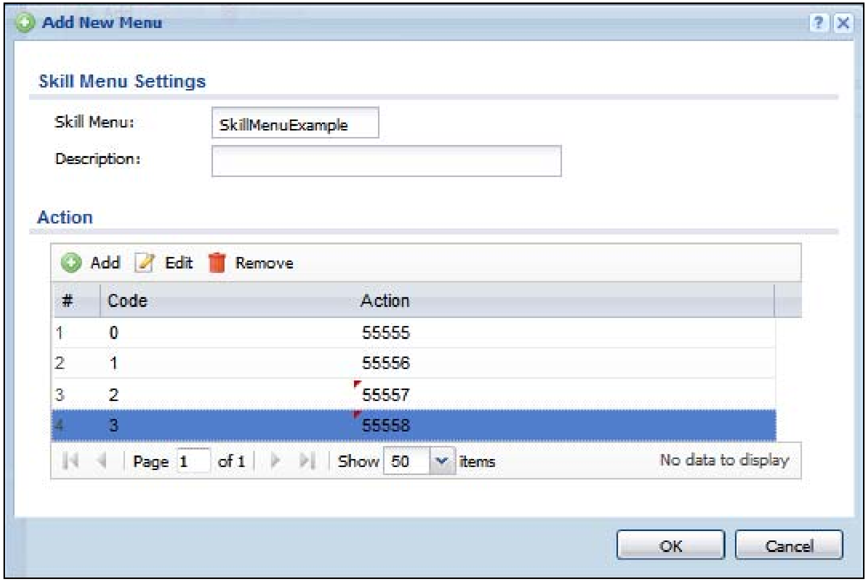
LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Skill Menu	This indicates the name for this skill menu.
Description	This indicates the description for this skill menu.

38.6.1 The Skill Menu Settings Screen

Use this screen to create or edit a skill menu.

Click either the **Add** or **Edit** icon in the **Skill Menu** screen to display the options as shown next.

Figure 379 Add Skill Menu



Skill Menu: SkillMenuExample

Description:

#	Code	Action
1	0	55555
2	1	55556
3	2	55557
4	3	55558

Each field is described in the following table.

Table 212 Add Skill Menu

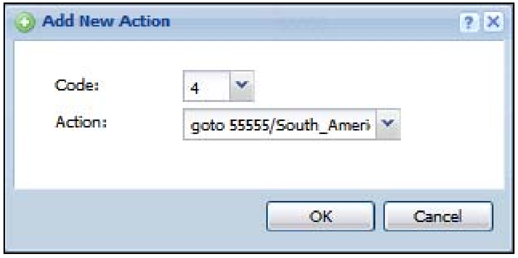
LABEL	DESCRIPTION
Skill Menu	Enter a name for this skill menu.
Description	Enter a description for this skill menu.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Code	This column indicates the keypad code that a caller can press to engage the associated action.
Action	This column indicates the action that happens when a caller presses an associated keypad code. The action is linked to the skills created on the **Configuration > PBX > ACD > Skill** screen.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

38.6.2 Add/Edit Skill Menu Action Screen

Use this screen to create or edit a skill menu action.

Click either the **Add** or **Edit** icons in the **Skill Menu Add** or **Edit** screen to display the options as shown next.

Figure 380 Add Skill Menu Action



Code: 4

Action: goto 55555/South_Ameri

Each field is described in the following table.

Table 213 Add Skill Menu Action

LABEL	DESCRIPTION
Code	Select a keypad code that a caller can press to engage the associated action. A single code can only be used once within a skill menu.
Action	Select an action that happens when a caller presses an associated keypad code. The action is linked to the skills created on the **Configuration > PBX > ACD > Skill** screen.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

39

Sound Files

You can upload sound files for different language menus. You can also

39.1 Overview

This chapter shows you how to change the language menus and some system sounds. You can also select the extension to record for creating audio files.

39.1.1 What You Can Do in this Chapter

- Use the **System Sound** screens to set the default language and upload sound files for different languages. See Section 39.2 on page 568.
- Use the **Specific Sound File** screens to upload custom recordings to play for specific PBX functions. See Section 39.3 on page 570.
- Use the **Record Peer** screen to select which extension to record from for creating audio files to use for the ISG50's PBX functions. See Section 39.4 on page 571.

39.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

System Language Sound File Formats

The audio files you upload must meet the following criteria:

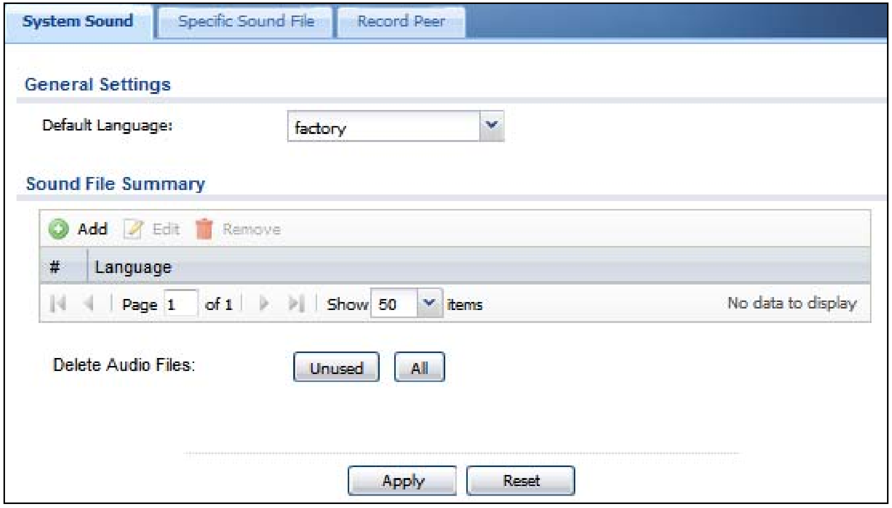
- G.722 format voice file (*.g722) or 16 kHz, 16-bit, PCM, mono mode format file (*.wav)
- The files should be zipped up in a single zip file per language.

39.2 The System Sound Screen

This screen allows you to set the default language and upload sound files for different languages.

Click **Configuration > PBX > Sound File** to open this screen.

Figure 381 Configuration > PBX > Sound File > System Sound


System Sound
Specific Sound File
Record Peer
General Settings
Sound File Summary
Add
Edit
Remove
#
Language
Page 1 of 1
Show 50 items
No data to display
Delete Audio Files:
Unused
All
Apply
Reset

Default Language: factory

Each field is described in the following table.

Table 214 Configuration > PBX > Sound File > System Sound

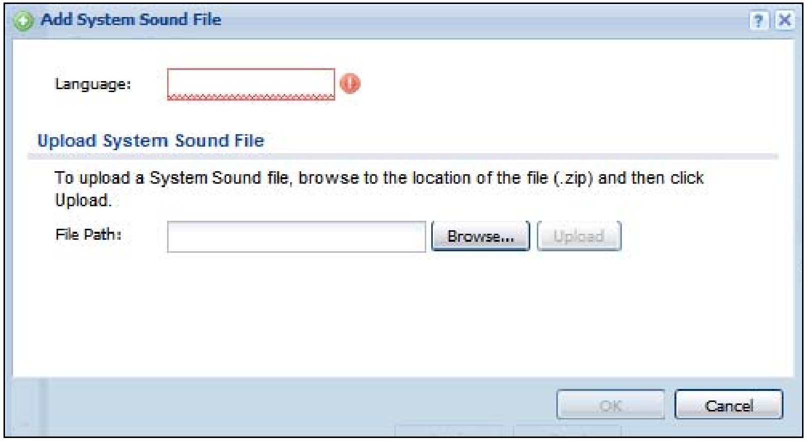
LABEL	DESCRIPTION
Default Language	Select the default language you want to use for the PBX functions.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Language	This indicates the name for this set of language sound files.
Delete Audio File	Click **Unused** to delete the language sound files that are not in the language list or **All** to delete all of the language sound files.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

39.2.1 The Add/Edit Sound File Screen

Use this screen to upload a language sound file.

Click either the **Add** or **Edit** icon in the **System Sound** screen to display the options as shown next.

Figure 382 Add System Sound File



Add System Sound File
Language:
Upload System Sound File
Browse...
Upload
OK
Cancel

To upload a System Sound file, browse to the location of the file (.zip) and then click Upload.

File Path:

Each field is described in the following table.

Table 215 Add System Sound File

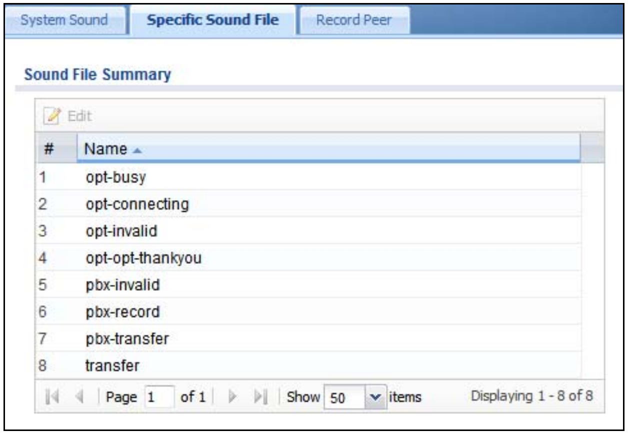
LABEL	DESCRIPTION
Language	Specify the name of the language sound files that you will upload.
Upload System Sound File	Click the **Browse** button to find the zipped set of language sound files on your computer that you want to upload. Click the **Upload** button to upload the selected file to the ISG50.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

39.3 The Specific Sound File Screen

This screen lists the specific PBX functions for which you can upload a customized audio file.

Click **Configuration > PBX > Sound File > Specific Sound File** to open this screen.

Figure 383 Configuration > PBX > Sound File > Specific Sound File



System Sound
Specific Sound File
Record Peer
Sound File Summary
Edit
Page 1 of 1
Show 50 items
Displaying 1 - 8 of 8

#	Name
1	opt-busy
2	opt-connecting
3	opt-invalid
4	opt-opt-thankyou
5	pbx-invalid
6	pbx-record
7	pbx-transfer
8	transfer

Each field is described in the following table.

Table 216 Configuration > PBX > Sound File > Specific Sound File

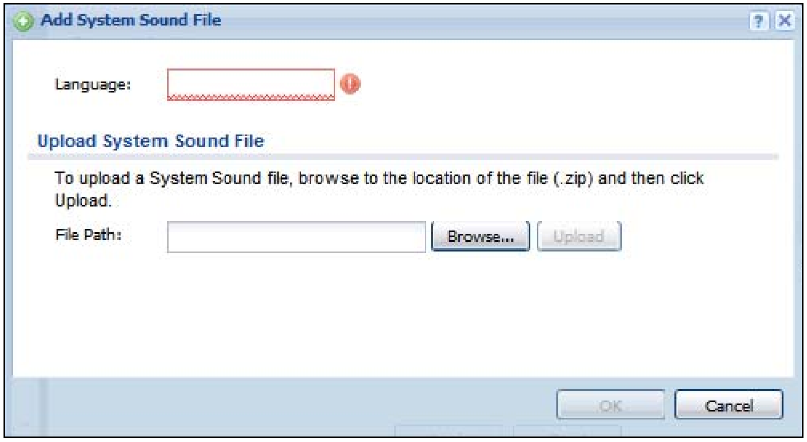
LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This indicates the name of the individual system sound.

39.3.1 The Add/Edit Sound File Screen

Use this screen to upload a language sound file.

Click either the **Add** or **Edit** icon in the **System Sound** screen to display the options as shown next.

Figure 384 Add System Sound File



To upload a System Sound file, browse to the location of the file (.zip) and then click Upload.

Each field is described in the following table.

Table 217 Add System Sound File

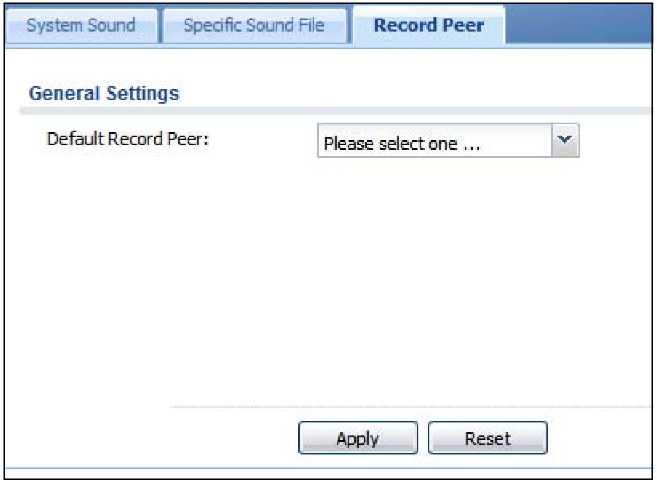
LABEL	DESCRIPTION
Language	Specify the name of the language sound files that you will upload.
Upload System Sound File	Click the **Browse** button to find the zipped set of language sound files on your computer that you want to upload. Click the **Upload** button to upload the selected file to the ISG50. The sound file must be 16-bit, 16 kHz, PCM, mono mode (*.wav).
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

39.4 The Record Peer Screen

Use the **Record Peer** screen to select which extension to record from for creating audio files to use for the ISG50's PBX functions.

Click **Configuration > PBX > Sound File > Record Peer** to open this screen.

Figure 385 Configuration > PBX > Sound File > Record Peer


System Sound
Specific Sound File
Record Peer
General Settings
Default Record Peer:
Please select one ...
Apply
Reset

Each field is described in the following table.

Table 218 Configuration > PBX > Sound File > Record Peer

LABEL	DESCRIPTION
Default Record Peer	Select the extension the ISG50 records from for creating audio files to use for the PBX functions.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

40

Auto Provision

40.1 Overview

This chapter shows you how to set up auto provisioning for the ISG50's supported SIP clients.

Auto provisioning allows administrators to configure VoIP related settings on snom or snom-compatible SIP clients from a central location. You can set up and maintain a configuration file associated with a SIP extension on the ISG50. Auto provisioning has the VoIP devices periodically download the configuration file from the ISG50.

Note: Check the documentation that came with your snom SIP client to see if it supports auto provisioning.

The configuration file contains the settings you configure for a specific telephone extension in your organization. It also contains SIP settings necessary for the device to register with the ISG50. The configuration file is encrypted using 3DES (Triple Data Encryption Standard). See Chapter 29 on page 453 for more information on extensions and Chapter 27 on page 429 for more information on SIP settings.

40.1.1 What You Can Do in this Chapter

- Use the **Auto Provision** screens to configure auto provisioning for the ISG50's supported SIP clients. See Section 40.2 on page 575.
- Use the **Auto Provision Advanced** screen to configure the feature key settings and firmware upgrade URLs for the snom VoIP devices connected to the ISG50. See Section 40.3 on page 578.

40.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

snom

A pioneer in the VoIP field, snom technology AG develops IP phones for use in corporate environments with an emphasis on quality, security and interoperability. As such, the ZyXEL ISG50 is designed to work as seamlessly as possible with a variety of snom products.

For more information, visit http://www.snom.com. If you have a snom product and are unsure how it works with auto provisioning, feature key settings, or firmware upgrades, consult the documentation that came with it.

How to Configure Auto Provisioning

Take the following steps to configure auto provisioning for the VoIP devices on your network. See also Section 8.2 on page 141 for an auto provisioning tutorial.

1. Configure SIP extensions that the snom VoIP devices will use. See Chapter 29 on page 453.
2. In the **Auto Provision** screen, map the SIP extensions to the MAC addresses of the snom VoIP devices by either adding the mappings manually or uploading a batch XML file. See Section 40.2 on page 575.
3. You can use the **Auto Provision Advance** screen to configure the feature key settings and firmware upgrade URLs for the snom VoIP devices connected to the ISG50 See Section 40.3 on page 578.
4. Configure the auto provisioning compliant snom devices to receive configuration information from the ISG50. This typically involves specifying the protocol used for auto provisioning. At the time of writing, you can use HTTP protocol for auto provisioning with the ISG50. See the documentation that came with your snom device for information on how to do this.

How Auto Provisioning Works

When a snom device is configured for auto provisioning, it attempts to use Simple Service Discovery Protocol (SSDP) to find the IP address of an auto provisioning server (for example the ISG50). This process is referred to as auto discovery.

Note: The auto discovery process is limited to your LAN.

Once a snom VoIP device finds the ISG50, it sends an HTTP request for a configuration file. The ISG50 checks to see if it has a configuration file associated with the serial number or MAC address of the snom device requesting the configuration file. If the ISG50 has the configuration file, then it sends the configuration file to the snom VoIP device.

You can also upload XML format files to the ISG50 for batch configuring ZyXEL’s IP phones.

40.1.3 Before You Begin

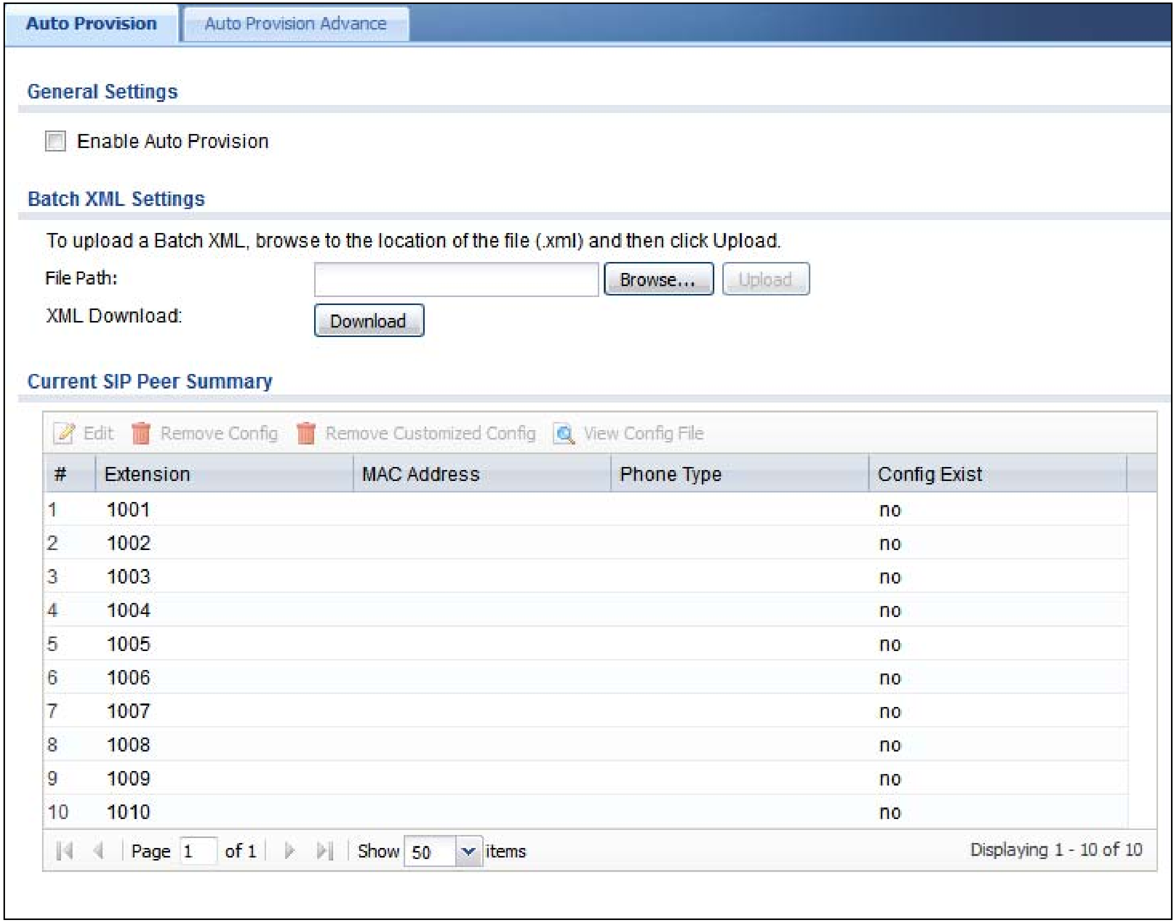
Before you start configuring Auto Provisioning on your ISG50, you should prepare the following:

- Create SIP extension(s) that you want to assign to your snom VoIP devices (see Section 29.2 on page 458).
- Find your snom VoIP devices’ MAC addresses on the devices’ back panel or package boxes. Use those to associate SIP numbers to your VoIP devices.

40.2 Auto Provision Setup

Use this screen to screens to configure auto provisioning for the snom VoIP devices connected to the ISG50. This screen displays the mapping between SIP extensions and snom VoIP device's MAC addresses. To access this screen, click **Configuration > PBX > Auto Provision**.

Figure 386 Configuration > PBX > Auto Provision


Auto Provision
Auto Provision Advance
General Settings
Batch XML Settings
Browse...
Upload
Download
Current SIP Peer Summary
Edit
Remove Config
Remove Customized Config
View Config File
Page 1 of 1
Show 50 items
Displaying 1 - 10 of 10

☐ Enable Auto Provision

To upload a Batch XML, browse to the location of the file (.xml) and then click Upload.

File Path:

XML Download:

#	Extension	MAC Address	Phone Type	Config Exist
1	1001			no
2	1002			no
3	1003			no
4	1004			no
5	1005			no
6	1006			no
7	1007			no
8	1008			no
9	1009			no
10	1010			no

Each field is described in the following table.

Table 219 Configuration > PBX > Auto Provision

LABEL	DESCRIPTION
Enable Auto Provision	Select this to turn on auto provisioning or clear it to turn it off.
Batch XML Settings	With the snom auto provision service enabled and at least one SIP extension configured, you can click **Download** to download a single XML configuration file. After you've downloaded the XML batch configuration file, you can edit it and use **Browse** and **Upload** to copy it to the ISG50.
Current SIP Peer Summary	Use this list to manage configuration files for the local snom VoIP devices.
Edit	Select an entry for an extension using a snom VoIP device and click the **Edit** icon to create a configuration file for it.
Remove Config	Select a snom VoIP device extension and click the **Remove Config** icon to remove its configuration profile.

Table 219 Configuration > PBX > Auto Provision (continued)

LABEL	DESCRIPTION
Remove Customized Config	Select a snom VoIP device extension and click the **Remove Config** icon to remove any custom configuration for it.
View Config File	Select a snom VoIP device extension and click the **View Config File** icon to view the configuration file for it or save a copy of the configuration file.
#	This field is a sequential value, and it is not associated with a specific entry.
Extension	This field displays the extension number configured on the ISG50.
MAC Address	This field displays the MAC address of the snom device specified to receive configuration settings from the ISG50. This field is blank for extensions assigned to non-snom VoIP SIP extensions.
Phone Type	This field displays the type of snom phone connected to the ISG50. This field is blank for extensions assigned to non-snom VoIP SIP extensions.
Config Exist	This field displays **Yes**, if there is a customized configuration file for the device or **No** if there is not.

40.2.1 snom Batch Configuration XML File

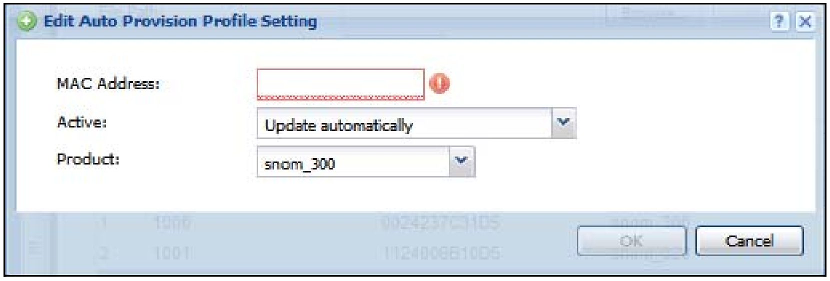
Here is an example of the snom batch configuration XML file.

```
<?xml version="1.0" encoding="utf-8"?>
<settings>
  <phone-settings e="2">
    <setting_server perm="RW">http://192.168.1.12:8080/provision/snom-lan-
{mac}.htm</setting_server>
    <update_policy perm="">auto_update</update_policy>
    <pnp_config perm="">on</pnp_config>
    <firmware_status perm="">http://192.168.1.12:8080/provision/
snom_300.xml</firmware_status>
    <user_active idx="1" perm="">on</user_active>
    <user_name idx="1" perm="">2222</user_name>
    <user_pname idx="1" perm="">2222</user_pname>
    <user_host idx="1" perm="">192.168.1.12</user_host>
    <user_hash idx="1" perm="">e5dd5800c7323de00c2f8f06173588c9</user_hash>
    <user_expiry idx="1" perm="">3600</user_expiry>
    <codec1_name idx="1" perm="">18</codec1_name>
    <codec2_name idx="1" perm="">0</codec2_name>
    <codec3_name idx="1" perm="">8</codec3_name>
    <codec4_name idx="1" perm="">2</codec4_name>
    <codec5_name idx="1" perm="">3</codec5_name>
    <codec6_name idx="1" perm="">18</codec6_name>
    <codec7_name idx="1" perm="">4</codec7_name>
    <user_dtmf_info idx="1" perm="">sip_info_only</user_dtmf_info>
    <user_dynamic_payload idx="1" perm="">off</user_dynamic_payload>
  </phone-settings>
</settings>
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%
```

40.2.2 Auto Provision Edit

Use this screen to set up the auto provisioning settings for a snom extension on the ISG50. To access this screen, click **Configuration > PBX > Auto Provision** and then click the **Edit** button for a snom device's extension.

Figure 387 Configuration > PBX > Auto Provision > Edit



MAC Address:

Active: Update automatically

Product: snom_300

Each field is described in the following table.

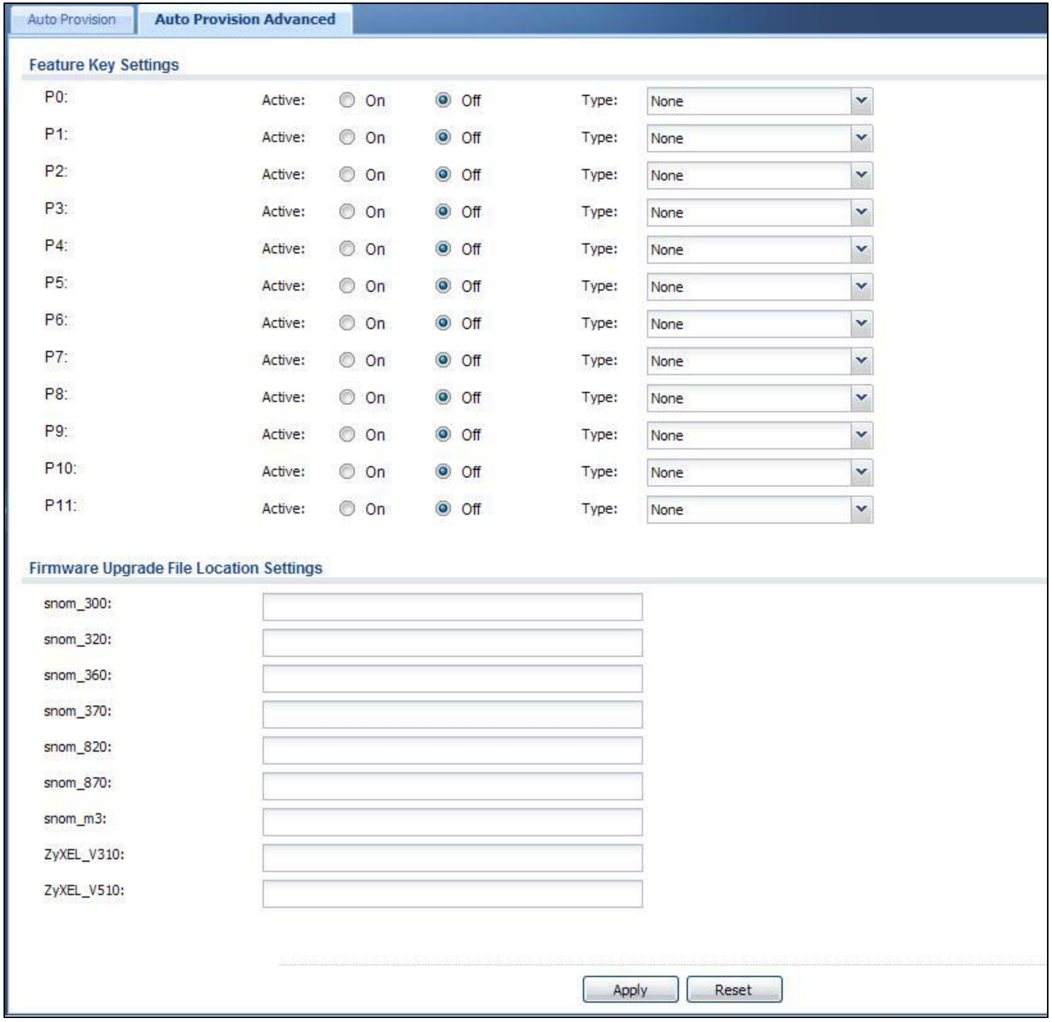
Table 220 Configuration > PBX > Auto Provision > Edit

LABEL	DESCRIPTION
MAC Address	Specify the MAC address of the snom device that receives configuration settings from the ISG50 for this extension.
Active	Select how to apply auto provisioning to this extension. • **Update automatically** - Automatically update this extension's firmware and/or configuration whenever an update of is available. • **Ask for update** - Update this extension's firmware and/or configuration whenever it checks for an update. • **Never update, load settings only** - Do not update this extension's firmware, only update its configuration. • **Never update, do not load settings** - Do not update this extension's firmware, and do not update its configuration.
Product	Select the snom VOIP product to be targeted by this auto provision profile. This ensures greater compatibility between it and the ISG50.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

40.3 Auto Provision Advanced Screen

Use this screen to configure the feature key settings and firmware upgrade URLs for the snom VoIP devices connected to the ISG50. To access this screen, click **Configuration > PBX > Auto Provision > Auto Provision Advanced** then click the **snom Feature Key Setting** button.

Figure 388 Configuration > PBX > Auto Provision > Auto Provision Advanced



Auto Provision
Auto Provision Advanced
Feature Key Settings
Firmware Upgrade File Location Settings
snom_300:
snom_320:
snom_360:
snom_370:
snom_820:
snom_870:
snom_m3:
ZyXEL_V310:
ZyXEL_V510:
Apply
Reset

P0:	Active:	○ On	● Off	Type: None
P1:	Active:	○ On	● Off	Type: None
P2:	Active:	○ On	● Off	Type: None
P3:	Active:	○ On	● Off	Type: None
P4:	Active:	○ On	● Off	Type: None
P5:	Active:	○ On	● Off	Type: None
P6:	Active:	○ On	● Off	Type: None
P7:	Active:	○ On	● Off	Type: None
P8:	Active:	○ On	● Off	Type: None
P9:	Active:	○ On	● Off	Type: None
P10:	Active:	○ On	● Off	Type: None
P11:	Active:	○ On	● Off	Type: None

Each field is described in the following table.

Table 221 Configuration > PBX > Auto Provision > Auto Provision Advanced

LABEL	DESCRIPTION
Feature Key Settings	This list corresponds to the special feature keys on a snom VoIP phone.
Active	Select either **On** or **Off** to enable or disable a key code for the feature key in question.
Type	Select a feature key action from this list. This only applies to the feature key if you made it active. For more information on feature key codes and their associated actions, see Section 27.3 on page 433.

Table 221 Configuration > PBX > Auto Provision > Auto Provision Advanced (continued)

LABEL	DESCRIPTION
Firmware Upgrade File Location Settings	This list corresponds to the snom products supported by the ISG50. Enter the firmware upgrade URL for the type of device. You can find this URL and any other upgrade information at the product page on the official snom website.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

41

Voice Mail

41.1 Overview

This chapter shows you how to set up voice mail for the ISG50's calls.

Voice mail messages on the ISG50 are stored on the built-in flash memory of the ISG50. To ensure that one user does not utilize a disproportionate amount of voice mail capacity, you can limit the per user voice mail resources on a system wide basis.

41.1.1 What You Can Do in this Chapter

Use the **Voice Mail** screen to set maximum call lengths per call or per user. See Section 41.2 on page 582.

41.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Voicemail Forwarding Method

You can manage your voice mail messages by forwarding them to email accounts associated with each telephone extension on the ISG50. See Chapter 29 on page 453 for information on how to configure email forwarding of voice mail messages.

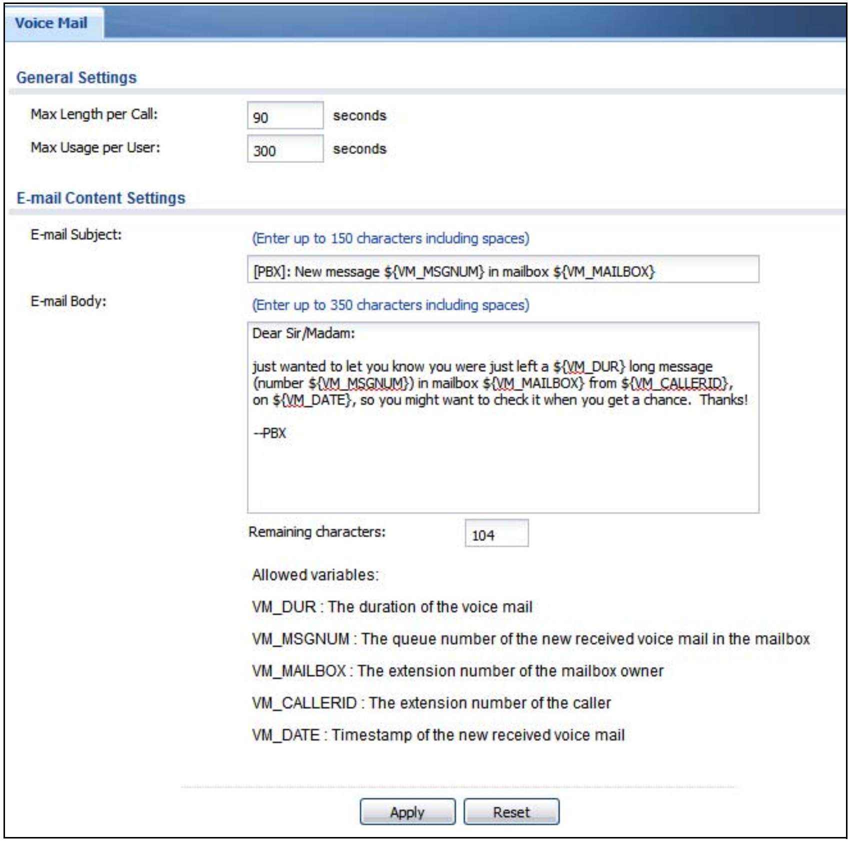
Access Personal Voice Mail

Users can access their personal voice mail system by dialing the feature code for voice mail (by default, ******) followed by their extension number. In the voice mail system, users can manage their personal voice messages, record their temporary greeting or messages which are played when they are unavailable or busy. See Section 41.3 on page 583.

41.2 The Voice Mail Screen

Use this screen to set up the voice mail settings on the ISG50. To access this screen, click **Configuration > PBX > Voice Mail**.

Figure 389 Configuration > PBX > Voice Mail



General Settings

Max Length per Call: 90 seconds

Max Usage per User: 300 seconds

E-mail Content Settings

E-mail Subject: (Enter up to 150 characters including spaces)

[PBX]: New message ${VM_MSGNUM} in mailbox ${VM_MAILBOX}

E-mail Body: (Enter up to 350 characters including spaces)

Dear Sir/Madam:

just wanted to let you know you were just left a ${VM_DUR} long message
(number ${VM_MSGNUM}) in mailbox ${VM_MAILBOX} from ${VM_CALLERID},
on ${VM_DATE}, so you might want to check it when you get a chance. Thanks!

--PBX

Remaining characters: 104

Allowed variables:

VM_DUR : The duration of the voice mail

VM_MSGNUM : The queue number of the new received voice mail in the mailbox

VM_MAILBOX : The extension number of the mailbox owner

VM_CALLERID : The extension number of the caller

VM_DATE : Timestamp of the new received voice mail

Each field is described in the following table.

Table 222 Configuration > PBX > Voice Mail

LABEL	DESCRIPTION
Max Length per Call	Specify the maximum number of seconds for each voice mail message. This value can be from 1 to 90 seconds.
Max Usage per User	Specify the maximum number of seconds for all voice mail messages for each extension. When a user hits this limit then the ISG50 will no longer save voice mail messages. This value can be from 1 to 600 seconds.
E-mail Subject	Enter up to 150 alphanumeric characters (a-z, A-Z, 1-0, all punctuation included) as the subject line for e-mails sent out by the ISG50 to notify users of pending voice mails.

Table 222 Configuration > PBX > Voice Mail (continued)

LABEL	DESCRIPTION
E-mail Body	Enter up to 350 alphanumeric characters (a-z, A-Z, 1-0, all punctuation included) as the body text for e-mails sent out by the ISG50 to notify users of pending voice mails. You can also use the following ISG50-specific variables to include custom information about the voice mail: • **VM_DUR**: This is the duration of the voice mail in hh:mm:ss format (hours, minutes, and seconds). • **VM_MSGNUM**: This is the queue number of the voice mail in the mailbox. The more voice mails you have received, the higher this number. • **VM_MAILBOX**: This is the telephone extension number of the mailbox owner. • **VM_CALLERID**: This is the telephone extension of the person who left the voice mail. • **VM_DATE**: This is the timestamp of when the voice mail was received.
Remaining characters	This field indicates the remaining number of characters available to you as you type your e-mail body text.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to set every field in this screen to its last-saved value.

41.3 Accessing Voice Mail

Users can access their personal voice mail system by dialing the feature code for voice mail followed by their extension number. The feature code for voice mail is configured in the **Configuration** > **PBX** > **Global** > **Feature Code** screen (see Section 27.3 on page 433). For example, if the feature code for voice mail is a double asterisks (******), then a caller (with extension **1001**) must dial ****1001** to access his personal voice mail system from any extension of the ISG50.

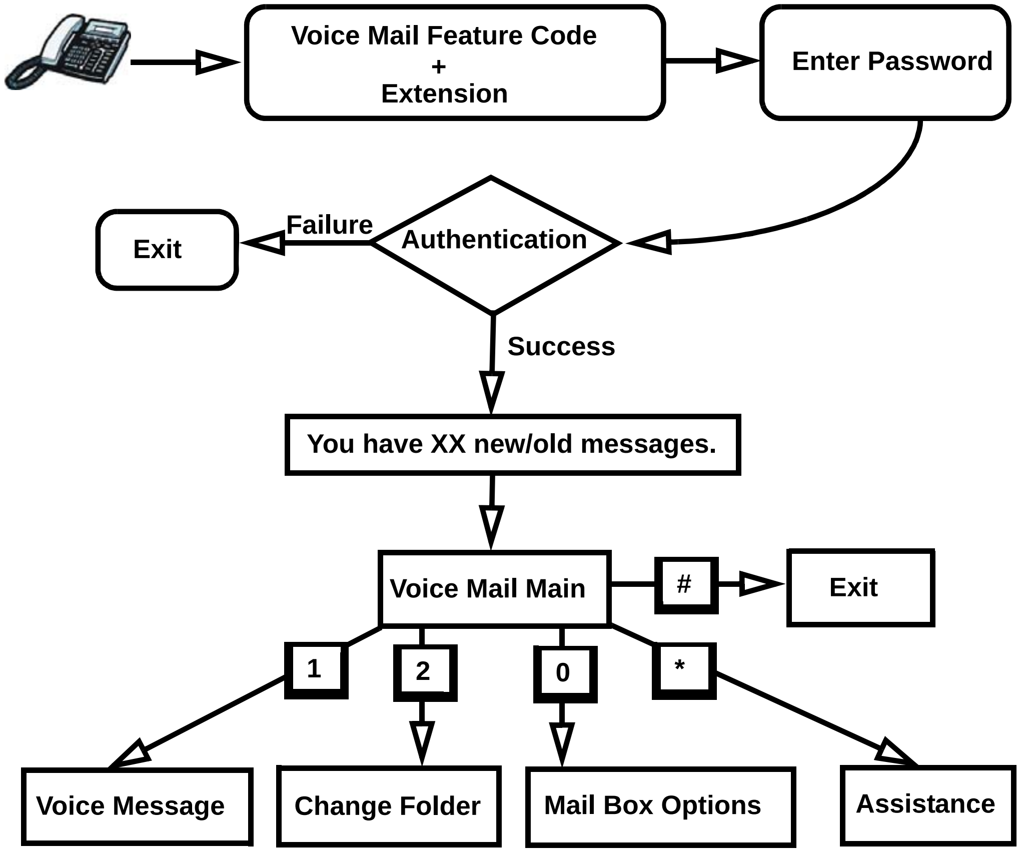
Personal voice mail can be accessed as an internal call or users can call from an outside line and dial the feature code for voice mail followed by their extension when an auto-attendant prompts them to dial the extension they wish to reach.

Users must authenticate before entering their voice mail system. When users dial into their personal voice mail they are prompted to enter their PIN. The voice mail PIN is assigned to each extension when the extension is created. See Section 29.3.1 on page 462 for information on how to configure the voice mail PIN for extensions. If a user authenticates successfully, the system prompts the number of new or old voice messages available for him or her in the system. Then he or she is guided through the personal voice mail menus via pre-recorded audio prompts. If a user fails to authenticate, the ISG50 plays a message indicating that an incorrect password was entered and the call is dropped after three trials.

Personal Voice Mail Main Flow

The following figure describes the main flow in the personal voice mail system.

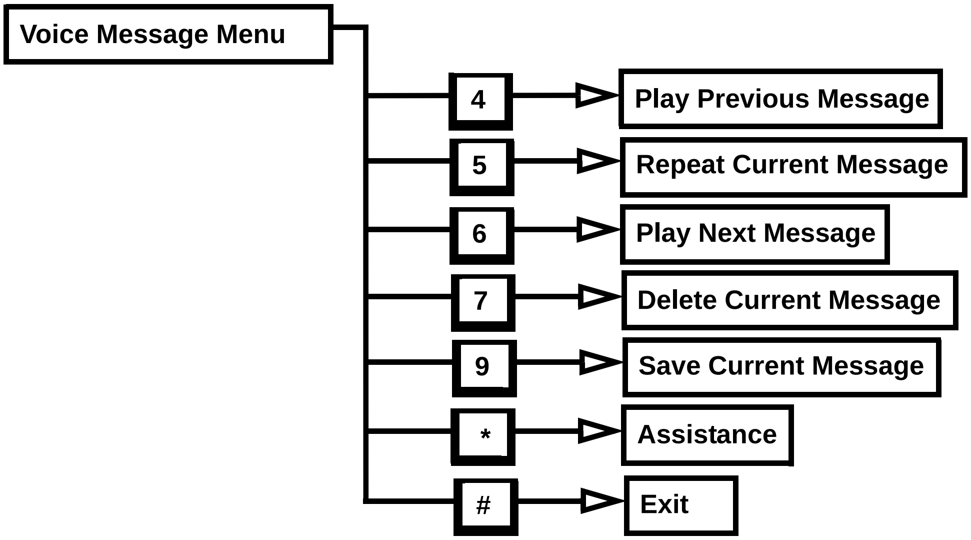
Figure 390 Personal Voice Mail Flow


Voice Mail Feature Code
+
Extension
Enter Password
Exit
Failure
Authentication
Success
You have XX new/old messages.
Voice Mail Main
#
Exit
1
2
0
*
Voice Message
Change Folder
Mail Box Options
Assistance

Voice Message Menu

The following figure describes the **Voice Message Menu**. From **Voice Mail Main**, press number **1** on your phone keypad to enter this menu. The ISG50 will play you a new message. Then you can choose either one of the following options for the next action.

Figure 391 Personal Voice Mail: Voice Message Menu

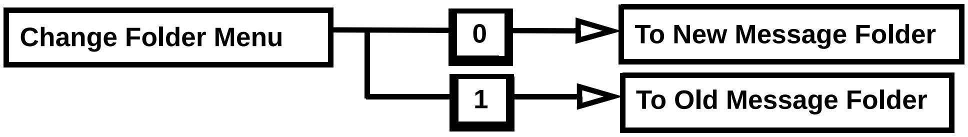

Voice Message Menu
4
Play Previous Message
5
Repeat Current Message
6
Play Next Message
7
Delete Current Message
9
Save Current Message
*
Assistance
#
Exit

If you press number **9** to save the current message, you can choose which folder to save it. The options are the same as the options in the **Change Folder Menu**. See Figure 392.

Change Folder Menu

The following figure describes the **Change Folder Menu**. From **Voice Mail Main**, press number **2** on your phone keypad to enter this menu. This menu allows you to switch the current folder to another folder in the voice mail system. Then system will play you the number of old messages stored in the folder to which you have switched. In this way, you can find an old message easily and replay it.

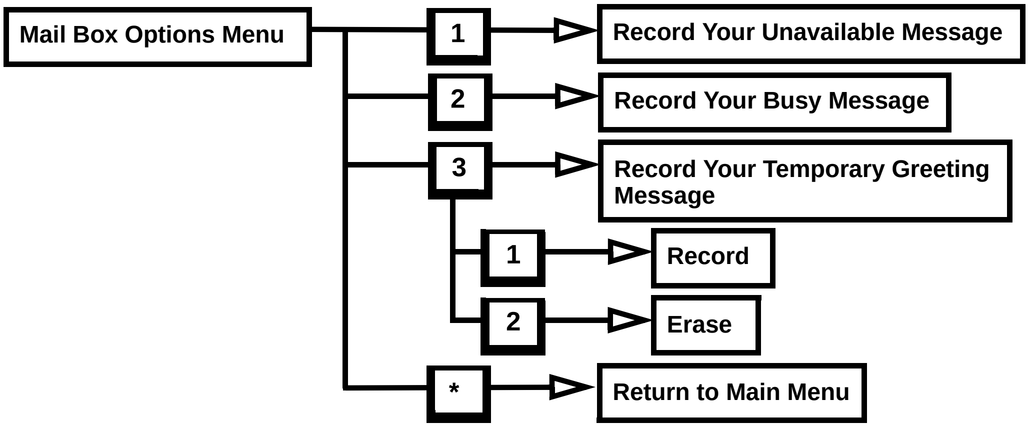
Figure 392 Personal Voice Mail: Change Folder Menu


Change Folder Menu
0
To New Message Folder
1
To Old Message Folder

Mail Box Options Menu

The following figure describes the **Mail Box Options Menu**. From **Voice Mail Main**, press number **0** on your phone keypad to enter this menu. This menu allows you to record your messages which are played for the initial greeting or when you (your extension) is unavailable, busy.

Figure 393 Personal Voice Mail: Mail Box Options Menu


Mail Box Options Menu
1
Record Your Unavailable Message
2
Record Your Busy Message
3
Record Your Temporary Greeting Message
1
Record
2
Erase
*
Return to Main Menu

After recording a message for unavailable, busy and/or temporary greeting, press the following number on your phone keypad to:

- 1 - accept what you recorded and save
- 2 - play what you recorded
- 3 - re-record the message

Voice Messages Storage

A voice message is stored as a .wav file and the size is about 8 KB per second. A storage of 64 MB can store messages recorded for about two hours in total.

42

Phonebook

42.1 Overview

This chapter shows you how to set up a phonebook for the ISG50.

There are two ways to set up a phone book on the ISG50.

- You can create an LDAP (Lightweight Directory Access Protocol) phonebook, which imports entries from an LDAP directory on your network.
- You can also create local phonebook entries via the web configurator of the ISG50.

You can configure either type of phonebook, or both. If you configure both phonebooks, then the entries from both phonebooks (duplicate entries included) are displayed to the end users.

42.1.1 What You Can Do in this Chapter

- Use the **General** screen to select which phonebooks the ISG50 transfers to the extensions. See Section 42.2 on page 588.
- Use the **LDAP Phonebook** screens to use phonebook entries from an LDAP directory on your network. See Section 42.3 on page 589.
- Use the **Local Phonebook** screen to import or export your local phonebook and manage the ISG50's local phonebook entries. See Section 42.5 on page 591.

42.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

LDAP Directories

LDAP directories are commonly used to store user based information within an organization. For example, email clients such as Outlook use LDAP to query address book entries from an LDAP directory. The ISG50 is capable of sending LDAP queries to an LDAP server to create and keep up-to-date the phone book entries on the ISG50.

The Local Phonebook

The local phonebook on the ISG50 can be created by adding phonebook entries via the web configurator. You can also export the local phonebook into a CSV format file. The text file can be edited and imported back to the ISG50 via the web configurator.

42.1.3 Before You Begin

If you intend to configure the ISG50 to use an LDAP phonebook, you need the following information about the LDAP server on your network to issue an LDAP query from the ISG50:

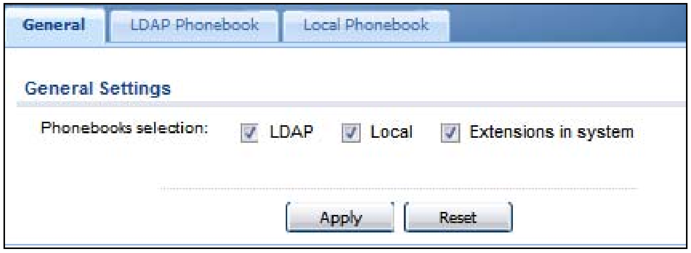
- LDAP Server IP address - this is the IP address of the LDAP server you want to query.
- Port number - this is the port number that the LDAP user to receive LDAP queries.
- RootDN - this is the username used to authenticate with the LDAP server. This information is configured on the LDAP server. Refer to your LDAP server documentation.
- Password - this is the password used to authenticate with the LDAP server.
- BaseDN - this string identifies the location on the LDAP server where the phone book information is stored. LDAP directories are divided into subdirectories and you need to enter the right subdirectory in order to search for the information for your phonebook.
- LDAP database field - these are names of the fields on the LDAP database that you want to obtain information from. Each record on the LDAP database contains many fields and you need to provide the correct field names in order to obtain the data.

42.2 The Phonebook General Screen

Use this screen to select which phonebooks the ISG50 transfers to the local extensions.

To access this screen, click **Configuration > PBX > Phonebook > General**.

Figure 394 Configuration > PBX > Phonebook > General



Phonebooks selection: ☑ LDAP ☑ Local ☑ Extensions in system

Each field is described in the following table.

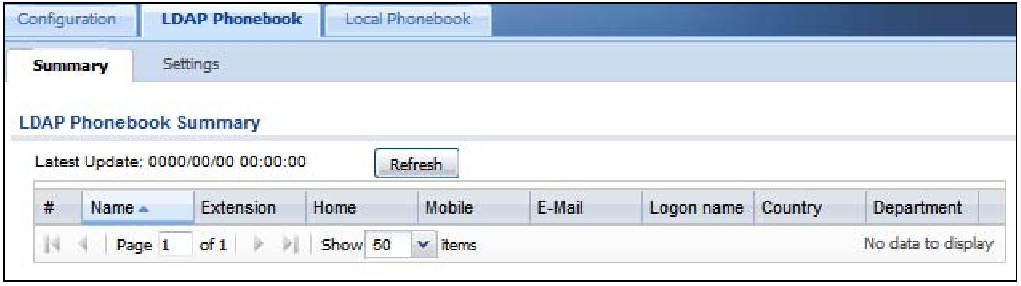
Table 223 Configuration > PBX > Phonebook > General

LABEL	DESCRIPTION
Phonebooks selection	Select which phonebooks to transfer to the local extensions. Select **LDAP** to transfer the LDAP server's account entries. Select **Local** to transfer the ISG50's phonebook. Select **Extensions in system** to transfer the ISG50's extensions.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

42.3 The LDAP Phonebook Summary Screen

Use this screen to view the phonebook entries retrieved from the LDAP database. To access this screen, click **Configuration > PBX > Phonebook** > **LDAP Phonebook**.

Figure 395 Configuration > PBX > Phonebook > LDAP Phonebook > Summary


Configuration
LDAP Phonebook
Local Phonebook
Summary
Settings
LDAP Phonebook Summary
Refresh
#
Name
Extension
Home
Mobile
E-Mail
Logon name
Country
Department
Page 1 of 1
Show 50 items
No data to display

Latest Update: 0000/00/00 00:00:00

Each field is described in the following table.

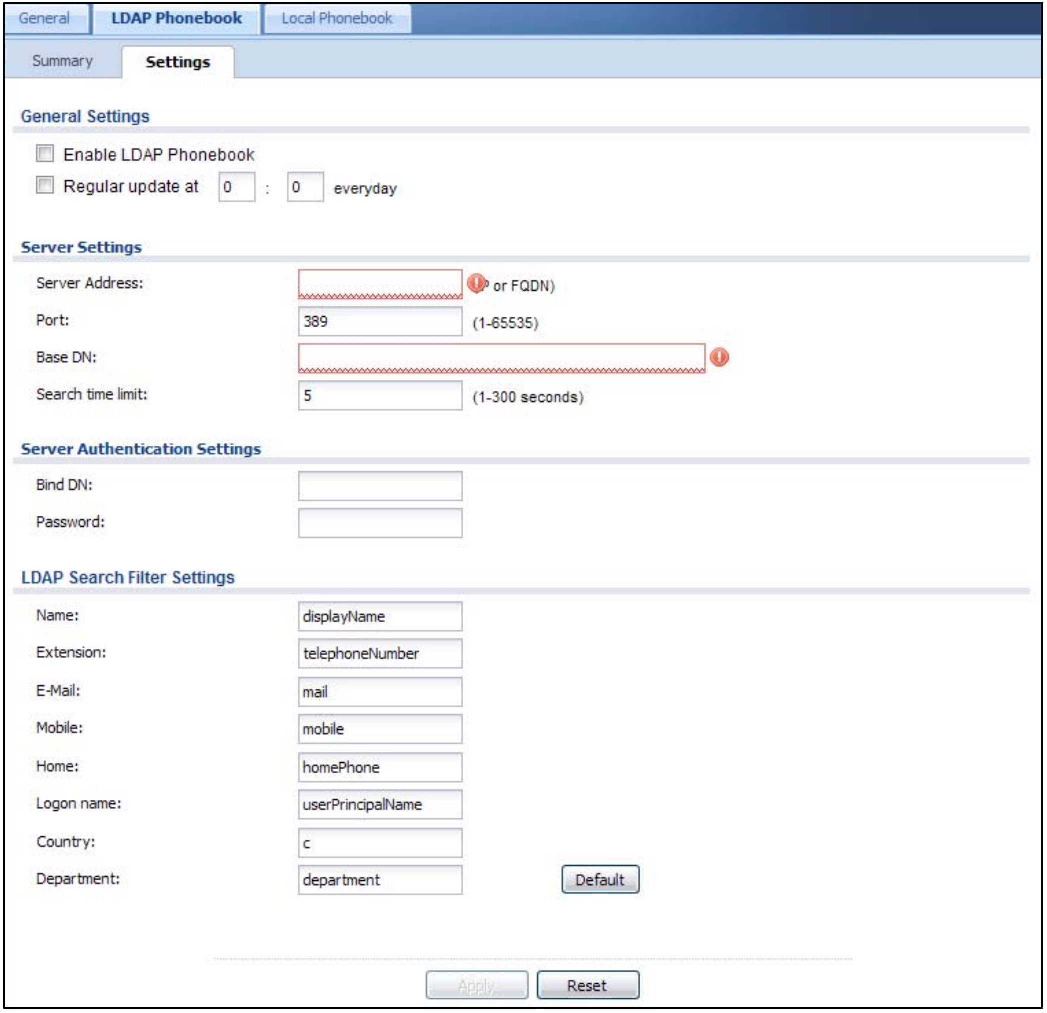
Table 224 Configuration > PBX > Phonebook > LDAP Phonebook > Summary

LABEL	DESCRIPTION
Refresh	Click **Refresh** to immediately update the LDAP phonebook with the LDAP database.
#	This field is a sequential value and is not associated with a specific entry.
Name	This field displays the **Name** field value of the local phonebook entry.
Extension	This field displays the **Extension** field value of the local phonebook entry.
Home	This field displays the **Home** field value of the local phonebook entry.
Mobile	This field displays the **Mobile** field value of the local phonebook entry.
E-Mail	This field displays the **E-Mail** field value of the local phonebook entry.
Logon name	This field displays the **Logon name** field value of the local phonebook entry.
Country	This field displays the **Country** field value of the local phonebook entry.
Department	This field displays the **Department** field value of the local phonebook entry.

42.4 The LDAP Phonebook Settings Screen

Use this screen to map the values associated with the account entries on the LDAP server to the phonebook values stored on the ISG50 and set up a connection to an LDAP server. You can also configure how often the ISG50 updates the LDAP phonebook from the LDAP server and configure the LDAP phonebook search filter. To access this screen, click **Configuration > PBX > Phonebook > LDAP Phonebook > Settings**.

Figure 396 Configuration > PBX > Phonebook > LDAP Phonebook > Settings



General Settings

☐ Enable LDAP Phonebook

☐ Regular update at 0 : 0 everyday

Server Settings

Server Address: or FQDN)

Port: 389 (1-65535)

Base DN:

Search time limit: 5 (1-300 seconds)

Server Authentication Settings

Bind DN:

Password:

LDAP Search Filter Settings

Name: displayName

Extension: telephoneNumber

E-Mail: mail

Mobile: mobile

Home: homePhone

Logon name: userPrincipalName

Country: c

Department: department

Each field is described in the following table.

Table 225 Configuration > PBX > Phonebook > LDAP Phonebook > Settings

LABEL	DESCRIPTION
Enable LDAP Phonebook	Check this box to enable LDAP based phonebook on the ISG50.
Regular update	Select this and specify the time in hour and minute format at which the ISG50 should update the LDAP phonebook with the LDAP database.
Server Address	Specify the address of the server containing the LDAP database.
Port	Specify the port the LDAP server uses for sending the phonebook to the ISG50.
Base DN	Enter the string identifying the location on the LDAP server where the information you need for your phonebook is stored.
Search time limit	Specify the longest that the ISG50 can attempt to connect to the LDAP server. If there is no response after this time, the ISG50 stops trying to connect and waits until the next day's update time.
Bind DN	Specify the login name of the LDAP server.

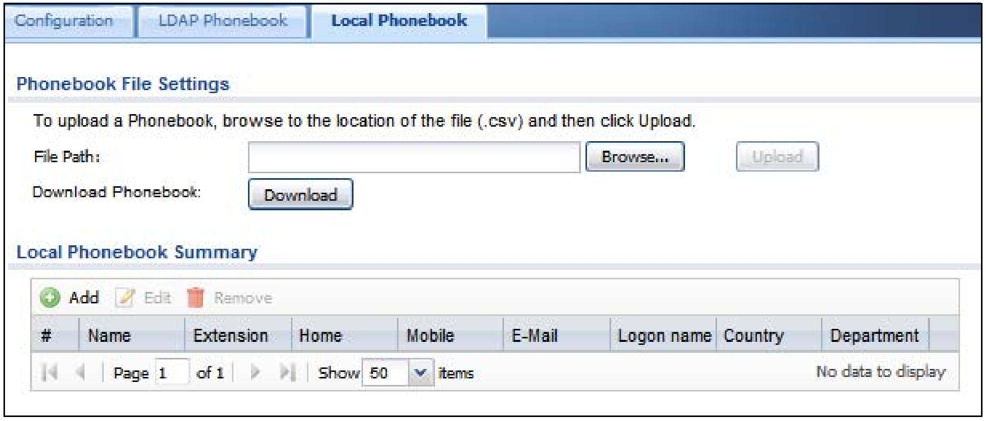
Table 225 Configuration > PBX > Phonebook > LDAP Phonebook > Settings (continued)

LABEL	DESCRIPTION
Password	Specify the password for the LDAP server.
Name	Specify the field name in the LDAP database that you want to map the **Name** field of the LDAP phonebook to.
Extension	Specify the field name in the LDAP database that you want to map the **Ext.** field of the LDAP phonebook to.
E-Mail	Specify the field name in the LDAP database that you want to map the **E-Mail** field of the LDAP phonebook to.
Mobile	Specify the field name in the LDAP database that you want to map the **Mobile** field of the LDAP phonebook to.
Home	Specify the field name in the LDAP database that you want to map the **Home** field of the LDAP phonebook to.
Logon Name	Specify the field name in the LDAP database that you want to map the **Logon Name** field of the LDAP phonebook to.
Country	Specify the field name in the LDAP database that you want to map the **Country** field of the LDAP phonebook to.
Department	Specify the field name in the LDAP database that you want to map the **Department** field of the LDAP phonebook to.
Default	Click **Default** to set every field in this section to the ISG50's factory defaults.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

42.5 The Local Phonebook Screen

Use this screen to import or export your local phonebook and manage the ISG50's local phonebook entries. To access this screen, click **Configuration > PBX > Phonebook > Local Phonebook**.

Figure 397 Configuration > PBX > Phonebook > Local Phonebook



To upload a Phonebook, browse to the location of the file (.csv) and then click Upload.

No data to display

Configuration
LDAP Phonebook
Local Phonebook
Phonebook File Settings
File Path:
Browse...
Upload
Download Phonebook:
Download
Local Phonebook Summary
Add
Edit
Remove
#
Name
Extension
Home
Mobile
E-Mail
Logon name
Country
Department
Page 1
of 1
Show 50
items

Each field is described in the following table.

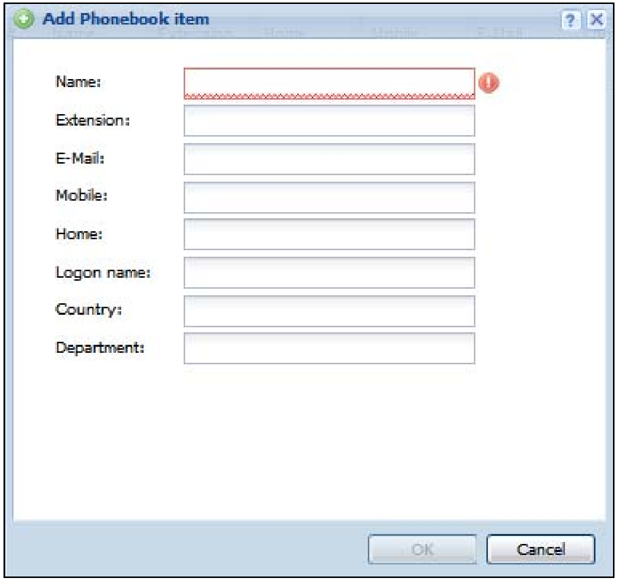
Table 226 Configuration > PBX > Phonebook > Local Phonebook

LABEL	DESCRIPTION
Phonebook File Settings	Use this section to upload a CSV format file containing your phonebook entries to the ISG50 or download the local phonebook from the ISG50 to your local computer or another location on your network.
File Path	Type the path to or click **Browse** and locate the text file containing a local phonebook. Then click **Upload** to upload the phonebook file to the ISG50.
Download Phonebook	Click **Download** to save the ISG50's local phonebook to your local computer or another location on your network. A screen appears prompting you for a location to download your phonebook file.
Local Phonebook Summary	This section allows you to view, add, edit and remove local phonebook entries on the ISG50.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value and is not associated with a specific entry.
Name	This field displays the **Name** field value of the local phonebook entry.
Extension	This field displays the **Extension** field value of the local phonebook entry.
Home	This field displays the **Home** field value of the local phonebook entry.
Mobile	This field displays the **Mobile** field value of the local phonebook entry.
E-Mail	This field displays the **E-Mail** field value of the local phonebook entry.
Logon name	This field displays the **Logon name** field value of the local phonebook entry.
Country	This field displays the **Country** field value of the local phonebook entry.
Department	This field displays the **Department** field value of the local phonebook entry.

42.5.1 Local Phonebook Add/Edit Screen

The screens for editing or adding entries to the local phonebook contain the same fields. Only the screen used to add local phonebook entries is shown below. Use this screen to configure phonebook entries on the ISG50. Click the **Add** (or **Edit**) icon in the **Local Phonebook** screen to view the screen as shown.

Figure 398 Local Phonebook Add/Edit Screen



Each field is described in the following table.

Table 227 Local Phonebook Add/Edit Screen

LABEL	DESCRIPTION
Name	Type a **Name** value for this local phonebook entry. You cannot change this value if you are editing an existing local phonebook entry.
Extension	Type an **Ext.** value for this local phonebook entry.
E-Mail	Type a **E-Mail** value for this local phonebook entry.
Mobile	Type a **Mobile** value for this local phonebook entry.
Home	Type a **Home** value for this local phonebook entry.
Logon name	Type a **Logon name** value for this local phonebook entry.
Country	Type a **country** value for this local phonebook entry.
Department	Type a **Department** value for this local phonebook entry.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

43

Office Hours

43.1 Overview

This chapter shows you how to set the office hours for the ISG50. You can use office hours to have the ISG50 deal with incoming calls differently at different times of day and night.

43.1.1 What You Can Do in this Chapter

Use the **Office Hour** screen to configure the days of the week and times you are in the office. See Section 43.2 on page 595.

43.1.2 What You Need To Know

The office hours you specify on the ISG50 are used by the auto-attendant feature to determine how the ISG50 handles incoming calls. For example, when calls come into your organization during office hours you may want to allow them to enter any extension they wish to call. However, when calls come into your organization after office hours you may want to direct them all to a single extension (a night clerk, for example).

43.1.3 Before You Begin

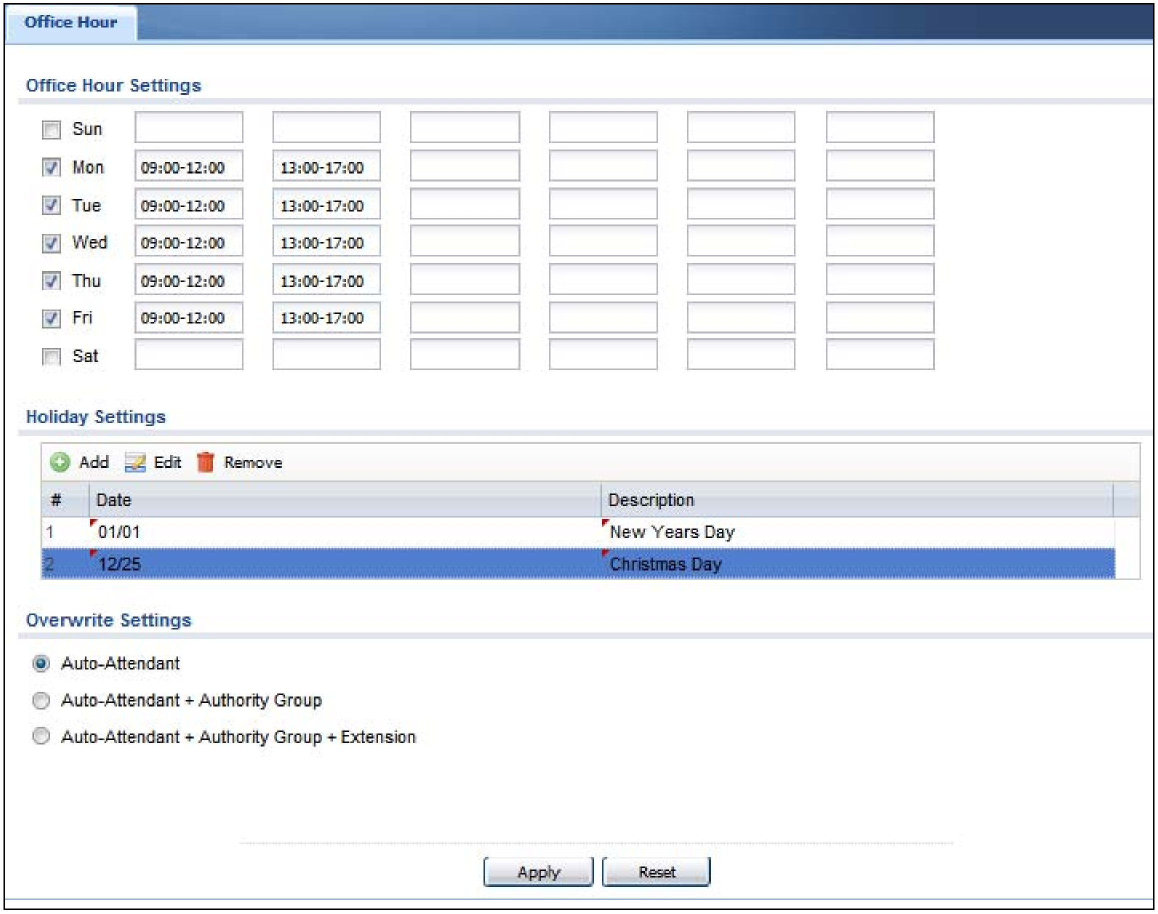
Before you configure office hours, you should know how to configure the auto-attendant. See Chapter 31 on page 503 for more information.

43.2 Office Hour Screen

Use this screen to specify office hours for the ISG50. To access this screen, click **Configuration > PBX > Office Hour**.

Note: The office hour configuration here is used as the default for all new extensions. To customize office hours on a per-extension or per-authority group basis, you must go to those specific screens. For more, see Chapter 29 on page 453.

Figure 399 Configuration > PBX > Office Hour



☐ Sun							
☑ Mon	09:00-12:00	13:00-17:00					
☑ Tue	09:00-12:00	13:00-17:00					
☑ Wed	09:00-12:00	13:00-17:00					
☑ Thu	09:00-12:00	13:00-17:00					
☑ Fri	09:00-12:00	13:00-17:00					
☐ Sat							

#	Date	Description
1	01/01	New Years Day
2	12/25	Christmas Day

● Auto-Attendant
○ Auto-Attendant + Authority Group
○ Auto-Attendant + Authority Group + Extension

Each field is described in the following table.

Table 228 Configuration > PBX > Office Hour

LABEL	DESCRIPTION
Office Hour Settings	Use this section to specify office hours on the ISG50.
Sun ~ Sat	Select the days of the week which you want the ISG50 to treat as working days. Specify the time range during the working days that you want the ISG50 to treat as working hours. When entering a time range, the following conditions apply: • You can enter up to six time ranges, with each range consisting of a start time and an end time. • The time entered in each field must be in 24 hour format (such as “08:00” for 8 AM or “13:00” for 1 PM). • The start and end times must be separated by a hyphen.
Holiday Settings	This section allows you to set a specific day of the year as a holiday, which the ISG50 will then treat as “after office hours”.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.

Table 228 Configuration > PBX > Office Hour (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value and is not associated with a specific entry.
Date	Enter a date in mm/dd format (double digit month / day; for example, 02/09 for February 9th.)
Description	Enter a description of the holiday.
Overwrite	Select an auto-attendant policy to be used for office hours: • **Auto-Attendant** - This applies the current system office hours to the auto-attendant. • **Auto-Attendant + Authority Group** - This applies the current system office hours to the auto-attendant and all authority groups. • **Auto-Attendant + Authority Group + Extension** - This applies the current system office hours to the auto-attendant, all authority groups, and all extensions.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

44

User/Group

44.1 Overview

This chapter describes how to set up user accounts, user groups, and user settings for the ISG50. You can also set up rules that control when users have to log in to the ISG50 before the ISG50 routes traffic for them.

44.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 44.2 on page 601) provides a summary of all user accounts.
- The **Group** screen (see Section 44.3 on page 604) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups
- The **Setting** screen (see Section 44.4 on page 605) controls default settings, login settings, lockout settings, and other user settings for the ISG50. You can also use this screen to specify when users must log in to the ISG50 before it routes traffic for them.

44.1.2 What You Need To Know

User Account

A user account defines the privileges of a user logged into the ISG50. User accounts are used in firewall rules, in addition to controlling access to configuration and services in the ISG50.

User Types

These are the types of user accounts the ISG50 uses.

Table 229 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change ISG50 configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at ISG50 configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 48 on page 631 for more information about authentication methods.)

Ext-User Accounts

Set up an **ext-user** account if the user is authenticated by an external server and you want to set up specific policies for this user in the ISG50. If you do not want to set up policies for this user, you do not have to set up an **ext-user** account.

All **ext-user** users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the ISG50 tries to use the local database to authenticate an **ext-user**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in Chapter 48 on page 631 and Chapter 49 on page 639, respectively.)

Note: If the ISG50 tries to authenticate an **ext-user** using the local database, the attempt always fails.

Once an **ext-user** user has been authenticated, the ISG50 tries to get the user type (see Table 229 on page 599) from the external server. If the external server does not have the information, the ISG50 sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the ISG50 checks the following places, in order.

1. User account in the remote server.
2. User account (Ext-User) in the ISG50.
3. Default user account for AD users (**ad-users**), LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the ISG50.

See Setting up User Attributes in an External Server on page 610 for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts work are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the AD or LDAP server. See Section 48.2.1 on page 635 for more on the group membership attribute.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the ISG50 to use the network services it provides. The ISG50 automatically routes packets for everyone. If you want to restrict network services that certain users can use via the ISG50, you can require them to log in to the ISG50 first. The ISG50 is then ‘aware’ of the user who is logged in and you can create ‘user-aware policies’ that define what services they can use. See Section 44.4.2 on page 609 for a user-aware login example.

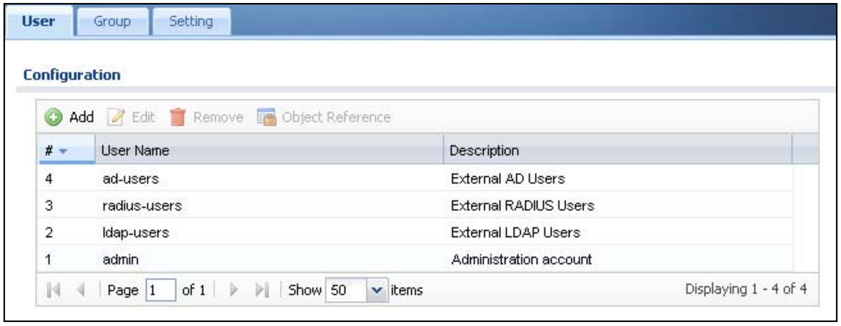
Finding Out More

- See Section 6.7.1 on page 104 for related information on these screens.
- See Section 44.5 on page 610 for some information on users who use an external authentication server in order to log in.
- See Section 7.5 on page 116 for an example of configuring user accounts and user groups as part of user-aware access control.
- See Section 7.6 on page 120 for an example of how to use a RADIUS server to authenticate user accounts based on groups.

44.2 User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group**.

Figure 400 Configuration > Object > User/Group



#	User Name	Description
4	ad-users	External AD Users
3	radius-users	External RADIUS Users
2	ldap-users	External LDAP Users
1	admin	Administration account

The following table describes the labels in this screen.

Table 230 Configuration > Object > User/Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	These are the entry numbers of the user accounts.
User Name	This field displays the user name of each user.
Description	This field displays the description for each user.

44.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

44.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

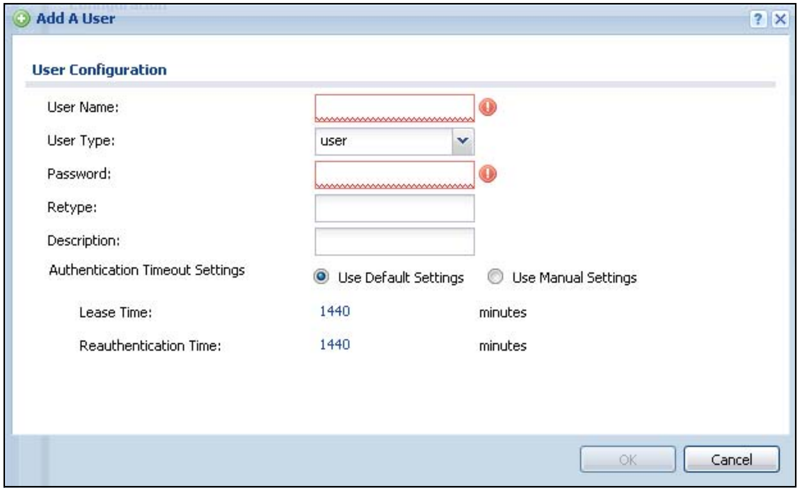
- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not ‘bob’.
- User names have to be different than user group names.
- Here are the reserved user names:
    - adm
    - admin
    - any
    - bin
    - daemon
    - debug
    - devicehaecived
    - ftp
    - games
    - halt
    - ldap-users
    - lp
    - mail
    - news
    - nobody
    - operator
    - radius-users
    - root
    - shutdown
    - sshd
    - sync
    - uucp
    - zyxel

To access this screen, go to the **User** screen (see Section 44.2 on page 601), and click either the **Add** icon or an **Edit** icon.

Figure 401 Configuration > User/Group > User > Add



User Configuration

User Name:
User Type: user
Password:
Retype:
Description:
Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings
Lease Time: 1440 minutes
Reauthentication Time: 1440 minutes

The following table describes the labels in this screen.

Table 231 Configuration > User/Group > User > Add

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 44.2.1.1 on page 602.
User Type	Select what type of user this is. Choices are: • **admin** - this user can look at and change the configuration of the ISG50 • **limited-admin** - this user can look at the configuration of the ISG50 but not to change it • **user** - this user has access to the ISG50's services but cannot look at the configuration • **guest** - this user has access to the ISG50's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 600 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 600 for more information about this type.
Password	This field is not available if you select the **ext-user** or **ext-group-user** type. Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters.
Retype	This field is not available if you select the **ext-user** or **ext-group-user** type.
Group Identifier	This field is available for a **ext-group-user** type user account. Specify the value of the AD or LDAP server's **Group Membership Attribute** that identifies the group to which this user belongs.
Associated AAA Server Object	This field is available for a **ext-group-user** type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	This field is not available if you select the **ext-group-user** type. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow.
Lease Time	This field is not available if you select the **ext-group-user** type. Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 44.4 on page 605), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	This field is not available if you select the **ext-group-user** type. Type the number of minutes this user can be logged into the ISG50 in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
Configuration Validation	Use a user account from the group specified above to test if the configuration is correct. Enter the account's user name in the **User Name** field and click **Test**.

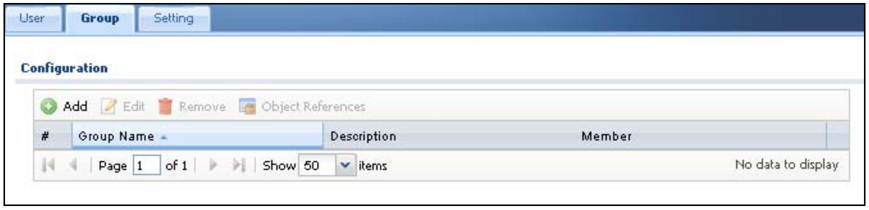
Table 231 Configuration > User/Group > User > Add (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

44.3 User Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Group**.

Figure 402 Configuration > Object > User/Group > Group



The following table describes the labels in this screen. See Section 44.3.1 on page 605 for more information as well.

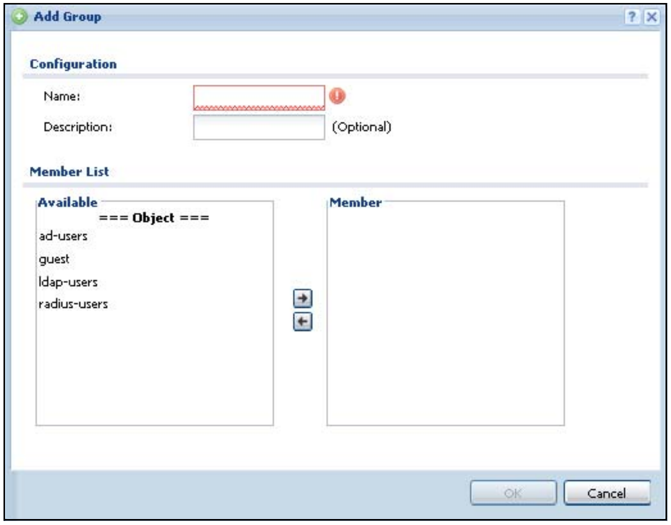
Table 232 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Removing a group does not remove the user accounts in the group.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.

44.3.1 Group Add/Edit Screen

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see Section 44.3 on page 604), and click either the **Add** icon or an **Edit** icon.

Figure 403 Configuration > User/Group > Group > Add



The following table describes the labels in this screen.

Table 233 Configuration > User/Group > Group > Add

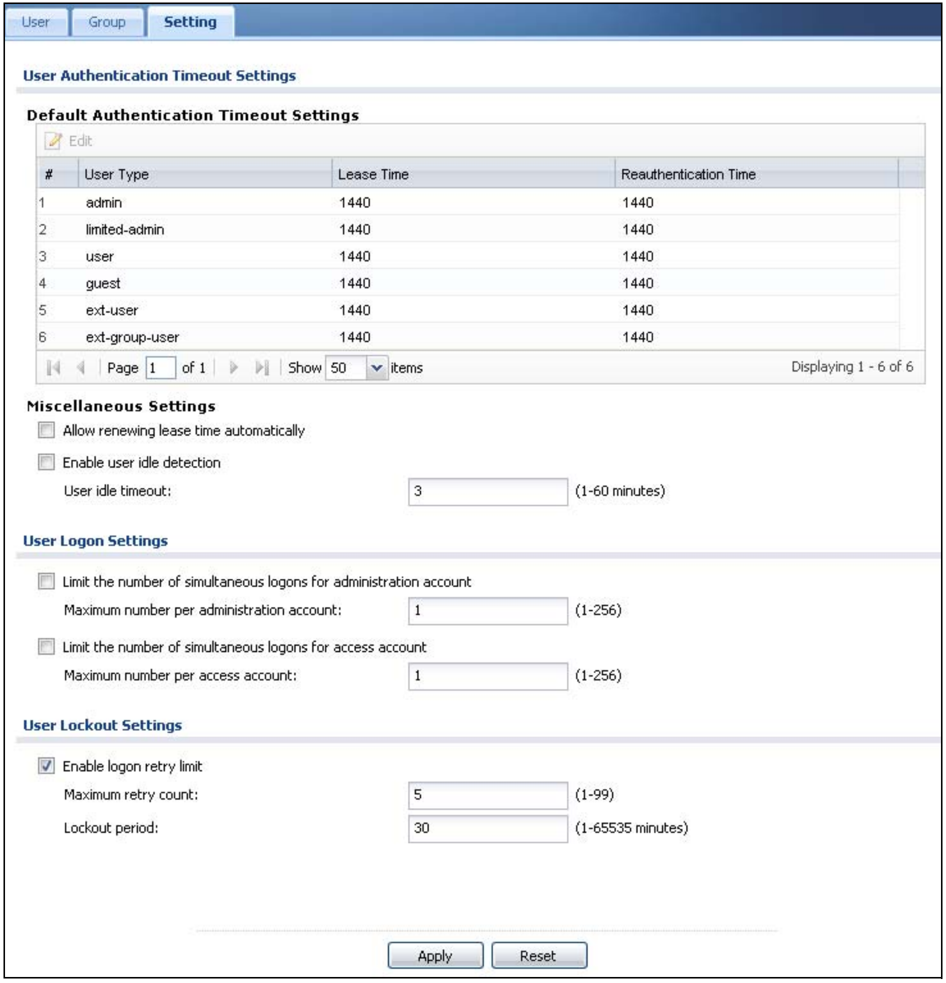
LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The **Member** list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the **Available** list that you want to be members of this group and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

44.4 Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the ISG50. You can also use this screen to specify when users must log in to the ISG50 before it routes traffic for them.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User/ Group > Setting**.

Figure 404 Configuration > Object > User/Group > Setting



User Authentication Timeout Settings

Default Authentication Timeout Settings

#	User Type	Lease Time	Reauthentication Time
1	admin	1440	1440
2	limited-admin	1440	1440
3	user	1440	1440
4	guest	1440	1440
5	ext-user	1440	1440
6	ext-group-user	1440	1440

Miscellaneous Settings

☐ Allow renewing lease time automatically

☐ Enable user idle detection

User idle timeout: 3 (1-60 minutes)

User Logon Settings

☐ Limit the number of simultaneous logons for administration account

Maximum number per administration account: 1 (1-256)

☐ Limit the number of simultaneous logons for access account

Maximum number per access account: 1 (1-256)

User Lockout Settings

☑ Enable logon retry limit

Maximum retry count: 5 (1-99)

Lockout period: 30 (1-65535 minutes)

The following table describes the labels in this screen.

Table 234 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Authentication Timeout Settings	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.

Table 234 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
User Type	These are the kinds of user account the ISG50 supports. • **admin** - this user can look at and change the configuration of the ISG50 • **limited-admin** - this user can look at the configuration of the ISG50 but not to change it • **user** - this user has access to the ISG50's services but cannot look at the configuration • **guest** - this user has access to the ISG50's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 600 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 600 for more information about this type.
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 44.4 on page 605), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the ISG50 in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
Miscellaneous Settings	
Allow renewing lease time automatically	Select this check box if access users can renew lease time automatically, as well as manually, simply by selecting the **Updating lease time automatically** check box on their screen.
Enable user idle detection	This is applicable for access users. Select this check box if you want the ISG50 to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The ISG50 automatically logs out the access user once the **User idle timeout** has been reached.
User idle timeout	This is applicable for access users. This field is effective when **Enable user idle detection** is checked. Type the number of minutes each access user can be logged in and idle before the ISG50 automatically logs out the access user.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user.
Limit the number of simultaneous logons for access account	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.

Table 234 Configuration > Object > User/Group > Setting (continued)

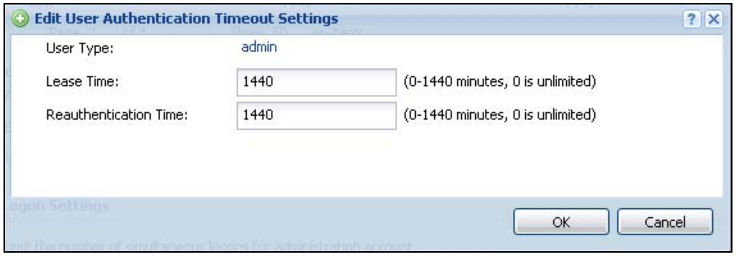
LABEL	DESCRIPTION
Maximum number per access account	This field is effective when **Limit ... for access account** is checked. Type the maximum number of simultaneous logins by each access user.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

44.4.1 Default User Authentication Timeout Settings Edit Screens

The **Default Authentication Timeout Settings Edit** screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User/Group > Setting** screen (see Section 44.4 on page 605), and click one of the **Default Authentication Timeout Settings** section's **Edit** icons.

Figure 405 Configuration > Object > User/Group > Setting > Edit



Edit User Authentication Timeout Settings

User Type: admin

Lease Time: 1440 (0-1440 minutes, 0 is unlimited)

Reauthentication Time: 1440 (0-1440 minutes, 0 is unlimited)

The following table describes the labels in this screen.

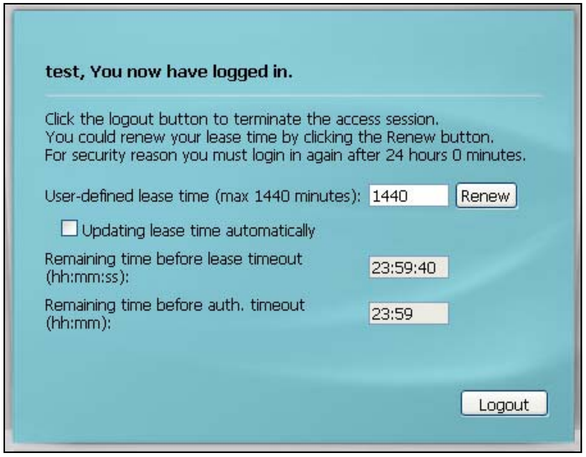
Table 235 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • **admin** - this user can look at and change the configuration of the ISG50 • **limited-admin** - this user can look at the configuration of the ISG50 but not to change it • **user** - this user has access to the ISG50's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 600 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 600 for more information about this type.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 44.4 on page 605), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the ISG50 in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

44.4.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the ISG50. Instead, after access users log into the ISG50, the following screen appears.

Figure 406 Web Configurator for Non-Admin Users



test, You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 24 hours 0 minutes.

User-defined lease time (max 1440 minutes): 1440

☐ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 23:59:40

Remaining time before auth. timeout (hh:mm): 23:59

The following table describes the labels in this screen.

Table 236 Web Configurator for Non-Admin Users

LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the ISG50 automatically logs them out. The ISG50 sets this amount of time according to the • **User-defined lease time** field in this screen • **Lease time** field in the **User Add/Edit** screen (see Section 44.2.1 on page 602) • **Lease time** field in the **Setting** screen (see Section 44.4 on page 605)
Updating lease time automatically	This box appears if you checked the **Allow renewing lease time automatically** box in the **Setting** screen. (See Section 44.4 on page 605.) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the **Renew** button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the ISG50 automatically logs the access user out, regardless of the lease time.

44.5 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 237 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	**User Type**. Possible Values: admin, limited-admin, user, guest.
leaseTime	**Lease Time**. Possible Values: 1-1440 (minutes).
reauthTime	**Reauthentication Time**. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 407 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 408 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts. See Chapter 55 on page 725 for more information about shell scripts.

45

Addresses

45.1 Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

45.1.1 What You Can Do in this Chapter

- The **Address** screen (Section 45.2 on page 613) provides a summary of all addresses in the ISG50. Use the **Address Add/Edit** screen to create a new address or edit an existing one.
- Use the **Address Group** summary screen (Section 45.3 on page 615) and the **Address Group Add/Edit** screen, to maintain address groups in the ISG50.

45.1.2 What You Need To Know

Address objects and address groups are used in dynamic routes, firewall rules, and VPN connection policies. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

- See Section 6.7 on page 103 for related information on these screens.
- See Section 7.11 on page 132 for how to create a public IP address range object for using multiple static public WAN IP addresses for LAN to WAN traffic.

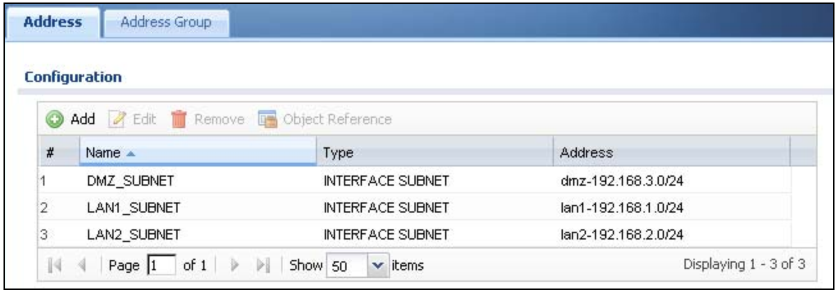
45.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.
- **SUBNET** - a network address is defined by a **Network** IP address and **Netmask** subnet mask.

The **Address** screen provides a summary of all addresses in the ISG50. To access this screen, click **Configuration > Object** > **Address > Address**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 409 Configuration > Object > Address > Address



#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
3	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

The following table describes the labels in this screen. See Section 45.2.1 on page 614 for more information as well.

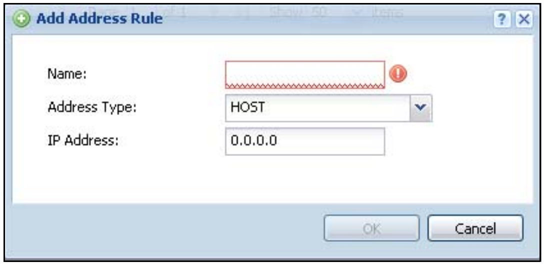
Table 238 Configuration > Object > Address > Address

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "**INTERFACE**" means the object uses the settings of one of the ISG50's interfaces.
Address	This field displays the IP addresses represented by each address object. If the object's settings are based on one of the ISG50's interfaces, the name of the interface displays first followed by the object's current address settings.

45.2.1 Address Add/Edit Screen

The **Configuration > Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 45.2 on page 613), and click either the **Add** icon or an **Edit** icon.

Figure 410 Configuration > Object > Address > Address > Edit



Name:
Address Type: HOST
IP Address: 0.0.0.0

The following table describes the labels in this screen.

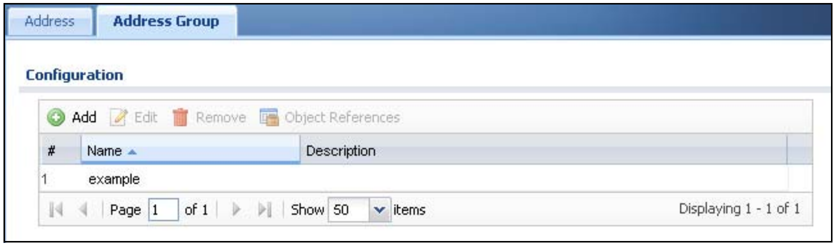
Table 239 Configuration > Object > Address > Address > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: **HOST**, **RANGE**, **SUBNET**, **INTERFACE IP**, **INTERFACE SUBNET**, and **INTERFACE GATEWAY**. Note: The ISG50 automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change **wan1**'s IP address, the ISG50 automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected **INTERFACE IP**, **INTERFACE SUBNET**, or **INTERFACE GATEWAY** as the **Address Type**, use this field to select the interface of the network that this address object represents.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

45.3 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Configuration > Object** > **Address > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 411 Configuration > Object > Address > Address Group



#	Name	Description
1	example	

The following table describes the labels in this screen. See Section 45.3.1 on page 616 for more information as well.

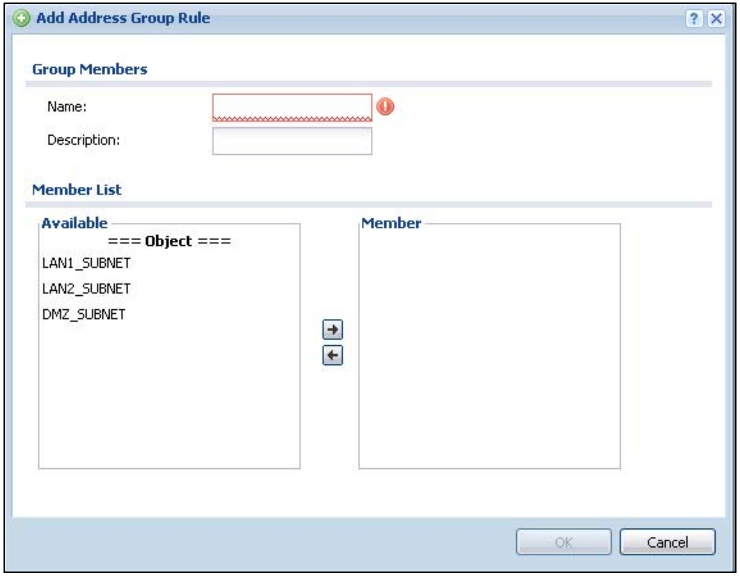
Table 240 Configuration > Object > Address > Address Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.

45.3.1 Address Group Add/Edit Screen

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see Section 45.3 on page 615), and click either the **Add** icon or an **Edit** icon.

Figure 412 Configuration > Object > Address > Address Group > Add



The following table describes the labels in this screen.

Table 241 Configuration > Object > Address > Address Group > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.

Table 241 Configuration > Object > Address > Address Group > Add (continued)

LABEL	DESCRIPTION
Member List	The **Member** list displays the names of the address and address group objects that have been added to the address group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

46

Services

46.1 Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

46.1.1 What You Can Do in this Chapter

- Use the **Service** screens (Section 46.2 on page 620) to view and configure the ISG50's list of services and their definitions.
- Use the **Service Group** screens (Section 46.2 on page 620) to view and configure the ISG50's list of service groups.

46.1.2 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes and firewall rules.

Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

Finding Out More

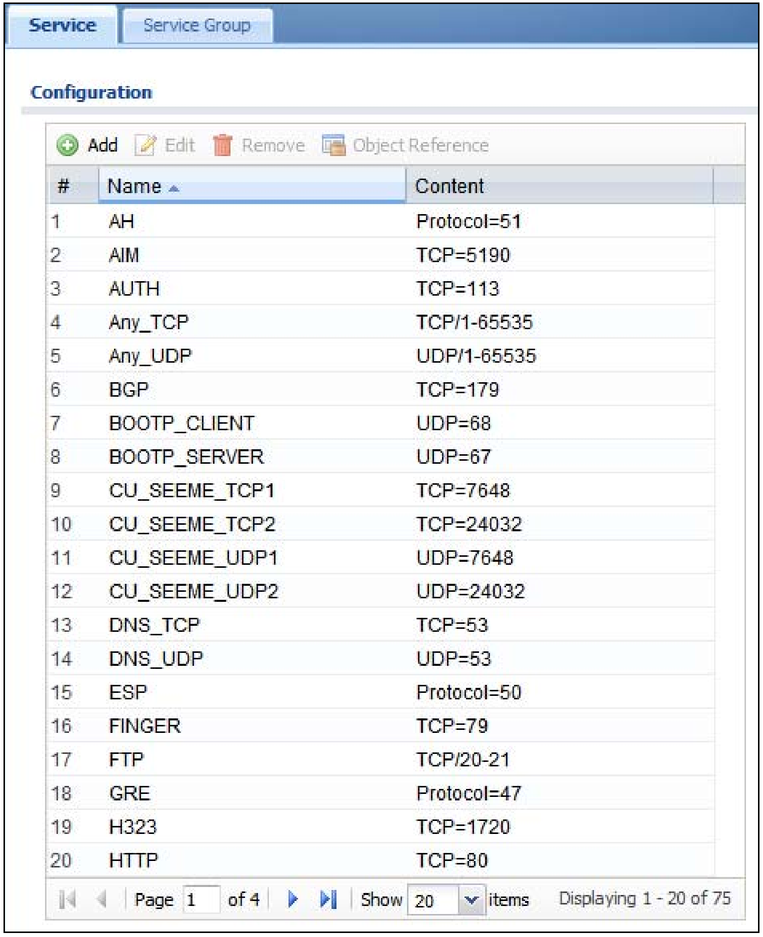
- See Section 6.7 on page 103 for related information on these screens.
- See Appendix B on page 827 for a list of commonly-used services.

46.2 The Service Summary Screen

The **Service** summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click **Configuration > Object > Service > Service**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 413 Configuration > Object > Service > Service



#	Name	Content
1	AH	Protocol=51
2	AIM	TCP=5190
3	AUTH	TCP=113
4	Any_TCP	TCP/1-65535
5	Any_UDP	UDP/1-65535
6	BGP	TCP=179
7	BOOTP_CLIENT	UDP=68
8	BOOTP_SERVER	UDP=67
9	CU_SEEME_TCP1	TCP=7648
10	CU_SEEME_TCP2	TCP=24032
11	CU_SEEME_UDP1	UDP=7648
12	CU_SEEME_UDP2	UDP=24032
13	DNS_TCP	TCP=53
14	DNS_UDP	UDP=53
15	ESP	Protocol=50
16	FINGER	TCP=79
17	FTP	TCP/20-21
18	GRE	Protocol=47
19	H323	TCP=1720
20	HTTP	TCP=80

The following table describes the labels in this screen.

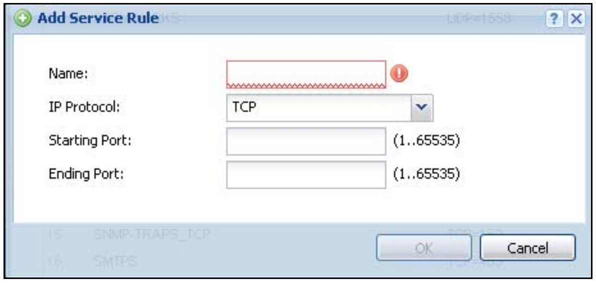
Table 242 Configuration > Object > Service > Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.

46.2.1 The Service Add/Edit Screen

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see Section 46.2 on page 620), and click either the **Add** icon or an **Edit** icon.

Figure 414 Configuration > Object > Service > Service > Edit



Name:
IP Protocol: TCP
Starting Port: (1..65535)
Ending Port: (1..65535)

The following table describes the labels in this screen.

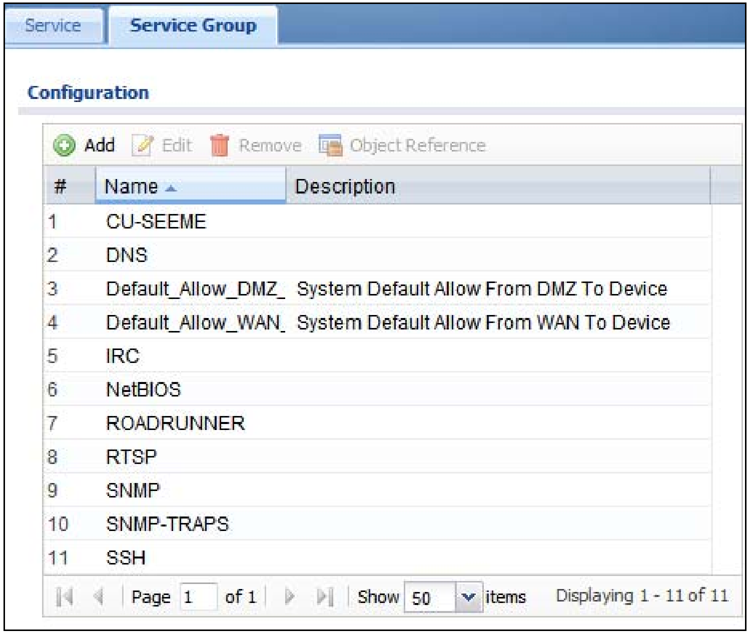
Table 243 Configuration > Object > Service > Service > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: **TCP**, **UDP**, **ICMP**, and **User Defined**.
Starting Port Ending Port	This field appears if the **IP Protocol** is **TCP** or **UDP**. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the **IP Protocol** is **ICMP Type**. Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the **IP Protocol** is **User Defined**. Enter the number of the next-level protocol (IP protocol). Allowed values are 0 - 255.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

46.3 The Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the Web Configurator, and click **Configuration > Object** > **Service** > **Service Group**.



#	Name	Description
1	CU-SEEME	
2	DNS	
3	Default_Allow_DMZ_	System Default Allow From DMZ To Device
4	Default_Allow_WAN_	System Default Allow From WAN To Device
5	IRC	
6	NetBIOS	
7	ROADRUNNER	
8	RTSP	
9	SNMP	
10	SNMP-TRAPS	
11	SSH	

Figure 415 Configuration > Object > Service > Service Group

The following table describes the labels in this screen. See Section 46.3.1 on page 624 for more information as well.

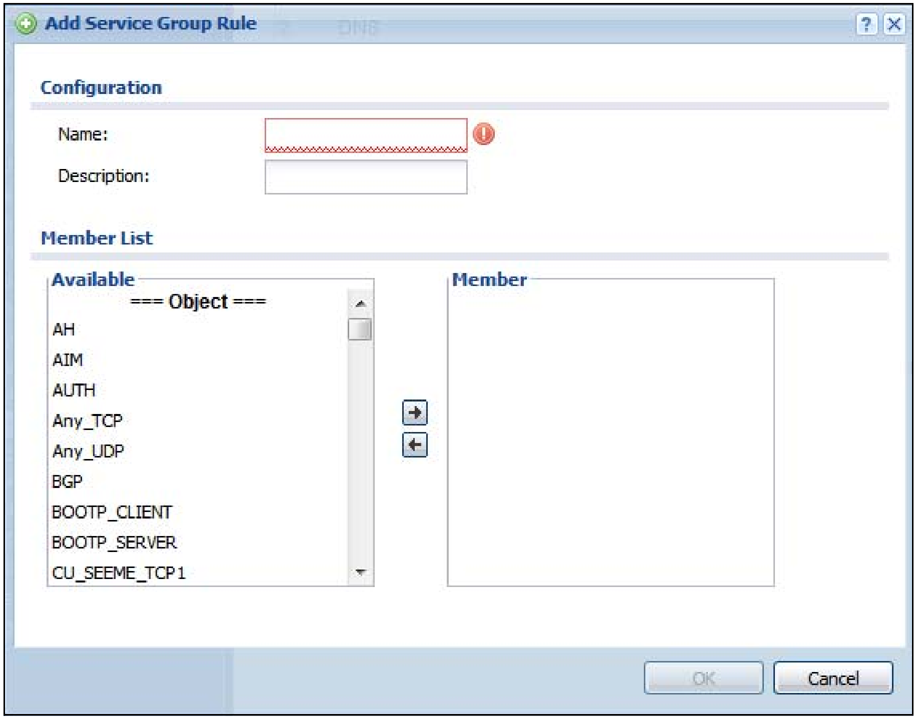
Table 244 Configuration > Object > Service > Service Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific service group.
Name	This field displays the name of each service group. By default, the ISG50 uses services starting with “Default_Allow_” in the firewall rules to allow certain services to connect to the ISG50.
Description	This field displays the description of each service group, if any.

46.3.1 The Service Group Add/Edit Screen

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see Section 46.3 on page 622), and click either the **Add** icon or an **Edit** icon.

Figure 416 Configuration > Object > Service > Service Group > Add


Add Service Group Rule
Configuration
Name:
Description:
Member List
Available
=== Object ===
AH
AIM
AUTH
Any_TCP
Any_UDP
BGP
BOOTP_CLIENT
BOOTP_SERVER
CU_SEEME_TCP1
Member
OK
Cancel

The following table describes the labels in this screen.

Table 245 Configuration > Object > Service > Service Group > Add

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	The **Member** list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

47

Schedules

47.1 Overview

Use schedules to set up one-time and recurring schedules for policy routes and firewall rules. The ISG50 supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ISG50.

Note: Schedules are based on the ISG50's current date and time.

47.1.1 What You Can Do in this Chapter

- Use the **Schedule** summary screen (Section 47.2 on page 626) to see a list of all schedules in the ISG50.
- Use the **One-Time Schedule Add/Edit** screen (Section 47.2.1 on page 627) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add/Edit** screen (Section 47.2.2 on page 628) to create or edit a recurring schedule.

47.1.2 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring Schedules

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

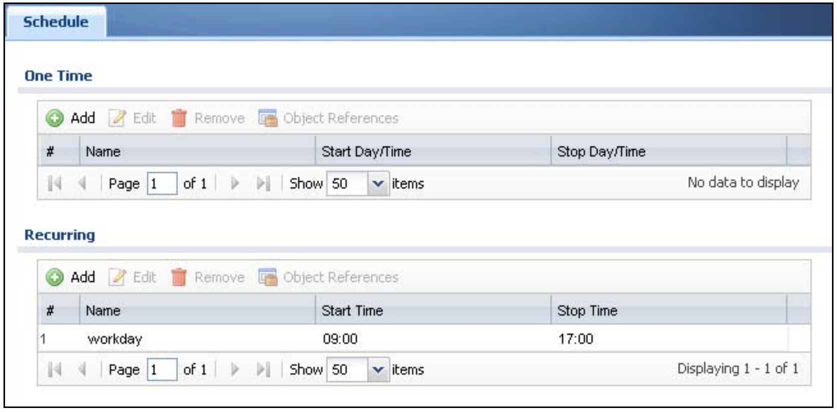
Finding Out More

- See Section 6.7 on page 103 for related information on these screens.
- See Section 52.4 on page 667 for information about the ISG50's current date and time.

47.2 The Schedule Summary Screen

The **Schedule** summary screen provides a summary of all schedules in the ISG50. To access this screen, click **Configuration > Object** > **Schedule**.

Figure 417 Configuration > Object > Schedule



#	Name	Start Day/Time	Stop Day/Time

No data to display

#	Name	Start Time	Stop Time
1	workday	09:00	17:00

Displaying 1 - 1 of 1

The following table describes the labels in this screen. See Section 47.2.1 on page 627 and Section 47.2.2 on page 628 for more information as well.

Table 246 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Recurring	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.

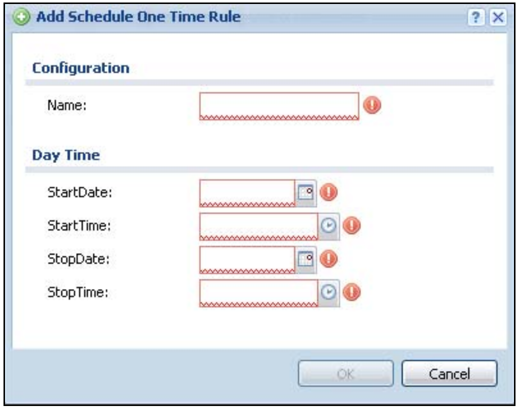
Table 246 Configuration > Object > Schedule (continued)

LABEL	DESCRIPTION
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.

47.2.1 The One-Time Schedule Add/Edit Screen

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 47.2 on page 626), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 418 Configuration > Object > Schedule > Add (One Time)



The following table describes the labels in this screen.

Table 247 Configuration > Object > Schedule > Add (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartDate	Specify the year, month, and day when the schedule begins. **Year** - 1900 - 2999 **Month** - 1 - 12 **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.) **Hour** - 0 - 23 **Minute** - 0 - 59
StartTime	Specify the hour and minute when the schedule begins. **Hour** - 0 - 23 **Minute** - 0 - 59

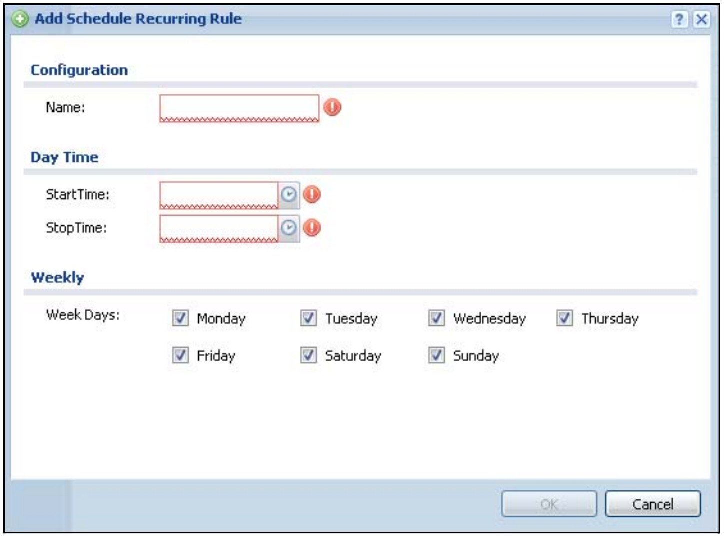
Table 247 Configuration > Object > Schedule > Add (One Time) (continued)

LABEL	DESCRIPTION
StopDate	Specify the year, month, and day when the schedule ends. **Year** - 1900 - 2999 **Month** - 1 - 12 **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.) **Hour** - 0 - 23 **Minute** - 0 - 59
StopTime	Specify the hour and minute when the schedule ends. **Hour** - 0 - 23 **Minute** - 0 - 59
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

47.2.2 The Recurring Schedule Add/Edit Screen

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 47.2 on page 626), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 419 Configuration > Object > Schedule > Add (Recurring)



Add Schedule Recurring Rule
Configuration
Name:
Day Time
StartTime:
StopTime:
Weekly
Week Days:
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday
OK
Cancel

The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

Table 248 Configuration > Object > Schedule > Add (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	

Table 248 Configuration > Object > Schedule > Add (Recurring) (continued)

LABEL	DESCRIPTION
StartTime	Specify the hour and minute when the schedule begins each day. **Hour** - 0 - 23 **Minute** - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. **Hour** - 0 - 23 **Minute** - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click **OK** to save your changes back to the ISG50.
Cancel	Click **Cancel** to exit this screen without saving your changes.

48

AAA Server

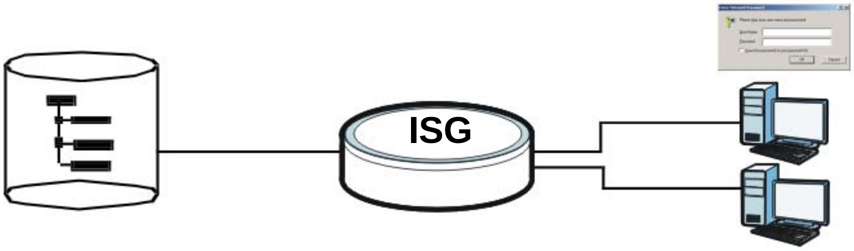
48.1 Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the **AAA Server** screens to create and manage objects that contain settings for using AAA servers. You use AAA server objects in configuring ext-group-user user objects and authentication method objects (see Chapter 49 on page 639).

48.1.1 Directory Service (AD/LDAP)

LDAP/AD allows a client (the ISG50) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 420 Example: Directory Service Client and Server



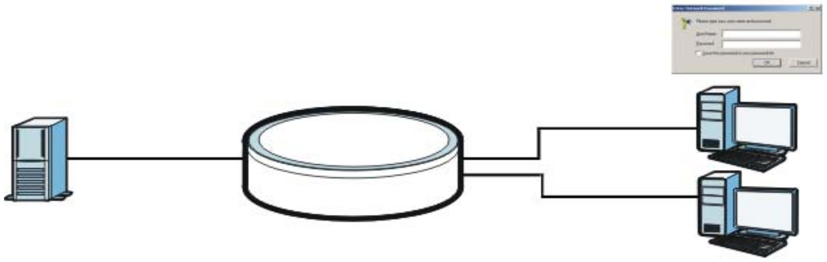
The following describes the user authentication procedure via an LDAP/AD server.

1. A user logs in with a user name and password pair.
2. The ISG50 tries to bind (or log in) to the LDAP/AD server.
3. When the binding process is successful, the ISG50 checks the user information in the directory against the user name and password pair.
4. If it matches, the user is allowed access. Otherwise, access is blocked.

48.1.2 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 421 RADIUS Server Network Example



48.1.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a ISG50 OTP package in order to use this feature. The package contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1. Install the ASAS server software on a computer.
2. Create user accounts on the ISG50 and in the ASAS server.
3. Import each token's database file (located on the included CD) into the server.
4. Assign users to OTP tokens (on the ASAS server).
5. Configure the ASAS as a RADIUS server in the ISG50's **Configuration > Object > AAA Server** screens.
6. Give the OTP tokens to (local or remote) users.

48.1.4 What You Can Do in this Chapter

- Use the **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) screens (Section 48.2 on page 634) to configure Active Directory or LDAP server objects.
- Use the **Configuration > Object > AAA Server > RADIUS** screen (Section 48.3 on page 636) to configure the default external RADIUS server to use for user authentication.

48.1.5 What You Need To Know

AAA Servers Supported by the ISG50

The following lists the types of authentication server the ISG50 supports.

- Local user database

  The ISG50 uses the built-in local user database to authenticate administrative users logging into the ISG50's Web Configurator or network access users logging into the network through the ISG50. You can also use the local user database to authenticate VPN users.

- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

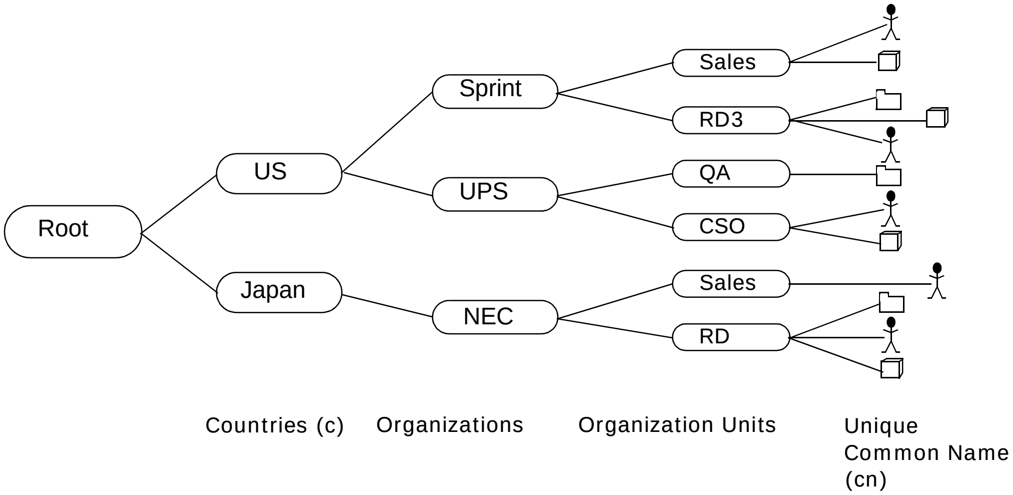
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 422 Basic Directory Structure



Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same "parent DN" ("`cn=domain1.com`, `ou=Sales, o=MyCompany`" in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, `o=MyCompany, c=UK` where `o` means organization and `c` means country.

Bind DN

A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of `cn=ISG50Admin` allows the ISG50 to log into the LDAP/AD server using the user name of `ISG50Admin`. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the ISG50 will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

Finding Out More

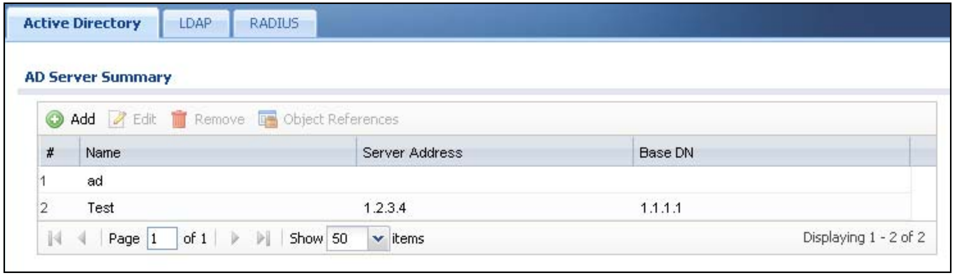
- See Section 7.5.3 on page 118 for an example of how to set up user authentication using a radius server.
- See Section 7.6 on page 120 for an example of how to use a RADIUS server to authenticate user accounts based on groups.

48.2 Active Directory or LDAP Server Summary

Use the **Active Directory** or **LDAP** screen to manage the list of AD or LDAP servers the ISG50 can use in authenticating users.

Click **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen.

Figure 423 Configuration > Object > AAA Server > Active Directory (or LDAP)



#	Name	Server Address	Base DN
1	ad		
2	Test	1.2.3.4	1.1.1.1

The following table describes the labels in this screen.

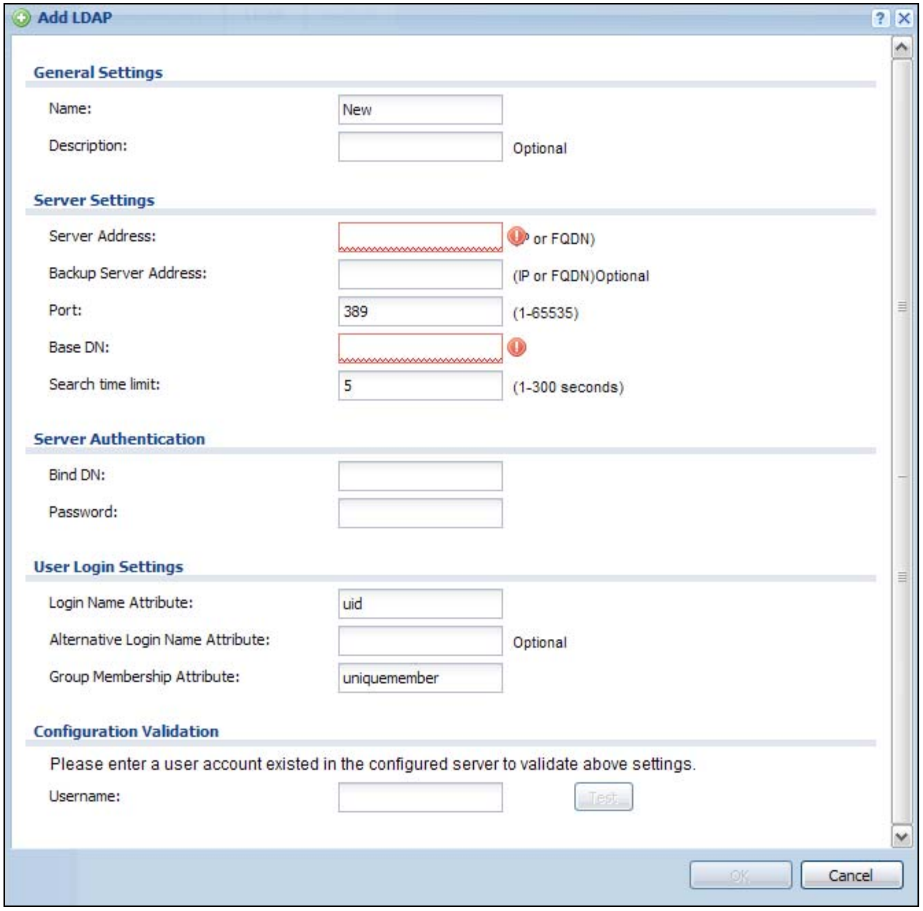
Table 249 Configuration > Object > AAA Server > Active Directory (or LDAP)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field displays the index number.
Name	This is the name of the AD or LDAP server entry.
Server Address	This is the address of the AD or LDAP server.
Base DN	This specifies a directory. For example, `o=ZyXEL, c=US`.

48.2.1 Adding an Active Directory or LDAP Server

Click **Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 424 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add


Add LDAP
General Settings
Description:
Optional
Server Settings
Server Address:
or FQDN)
Backup Server Address:
(IP or FQDN)Optional
Base DN:
Server Authentication
Bind DN:
Password:
User Login Settings
Alternative Login Name Attribute:
Optional
Configuration Validation
Username:
Test
OK
Cancel

Name: New

Port: 389 (1-65535)

Search time limit: 5 (1-300 seconds)

Login Name Attribute: uid

Group Membership Attribute: uniquemember

Please enter a user account existed in the configured server to validate above settings.

The following table describes the labels in this screen.

Table 250 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the AD or LDAP server.
Backup Server Address	If the AD or LDAP server has a backup server, enter its address here.
Port	Specify the port number on the AD or LDAP server to which the ISG50 sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, o=ZyXEL, c=US.

Table 250 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

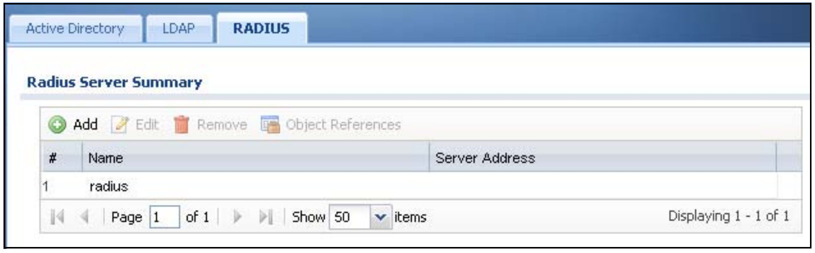
LABEL	DESCRIPTION
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the ISG50 disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters. For example, `cn=ISG50Admin` specifies `ISG50Admin` as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the ISG50 to bind (or log in) to the AD or LDAP server.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, `o=ZyXEL, c=US`.
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example "name" or "e-mail address".
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example "name" or "e-mail address".
Group Membership Attribute	An AD or LDAP server defines attributes for its accounts. Enter the name of the attribute that the ISG50 is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add **ext-group-user** user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a **ext-group-user** user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
Configuration Validation	Use a user account from the server specified above to test if the configuration is correct. Enter the account's user name in the **Username** field and click **Test**.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

48.3 RADIUS Server Summary

Use the **RADIUS** screen to manage the list of RADIUS servers the ISG50 can use in authenticating users.

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen.

Figure 425 Configuration > Object > AAA Server > RADIUS



Radius Server Summary

#	Name	Server Address
1	radius	

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

The following table describes the labels in this screen.

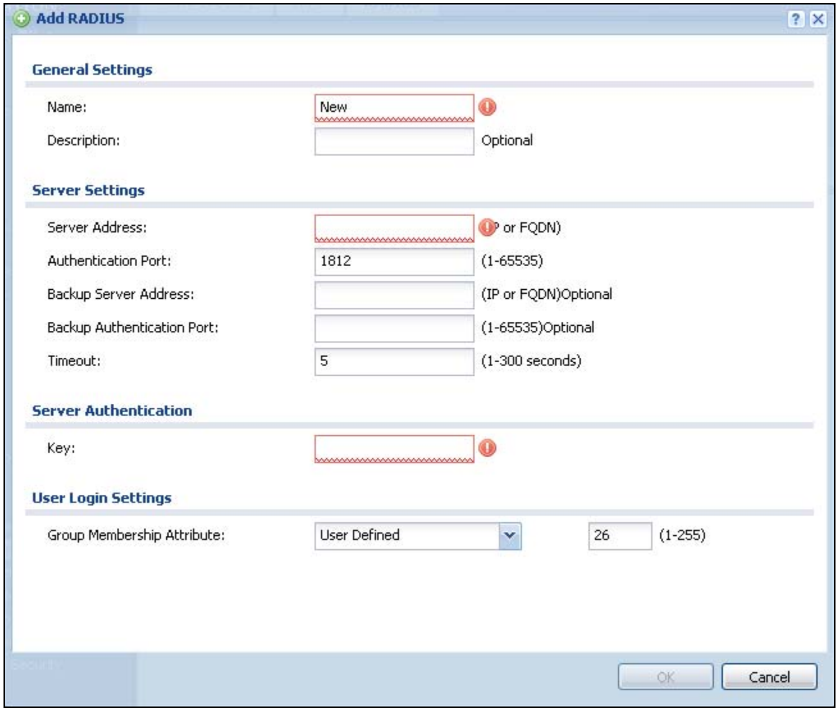
Table 251 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the RADIUS server.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

48.3.1 Adding a RADIUS Server

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 426 Configuration > Object > AAA Server > RADIUS > Add



Add RADIUS

General Settings

Name: New

Description: Optional

Server Settings

Server Address: P or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN)Optional

Backup Authentication Port: (1-65535)Optional

Timeout: 5 (1-300 seconds)

Server Authentication

Key:

User Login Settings

Group Membership Attribute: User Defined 26 (1-255)

The following table describes the labels in this screen.

Table 252 Configuration > Object > AAA Server > RADIUS > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the ISG50 sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the ISG50 sends authentication requests. Enter a number between 1 and 65535.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the ISG50 disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the ISG50. The key is not sent over the network. This key must be the same on the external authentication server and the ISG50.
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the ISG50 is to check to determine to which group a user belongs. If it does not display, select user-defined and specify the attribute's number. This attribute's value is called a group identifier; it determines to which group a user belongs. You can add **ext-group-user** user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a **ext-group-user** user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

49

Authentication Method

49.1 Overview

Authentication method objects set how the ISG50 authenticates wireless, HTTP/HTTPS clients, and peer IPSec routers (extended authentication) clients. Configure authentication method objects to have the ISG50 use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the ISG50 are authenticated locally.

49.1.1 What You Can Do in this Chapter

- Use the **Configuration > Object > Auth. Method** screens (Section 49.2 on page 640) to create and manage authentication method objects.

Finding Out More

See Section 7.5.3 on page 118 for an example of how to set up user authentication using a radius server.

49.1.2 Before You Begin

Configure AAA server objects (see Chapter 48 on page 631) before you configure authentication method objects.

49.1.3 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

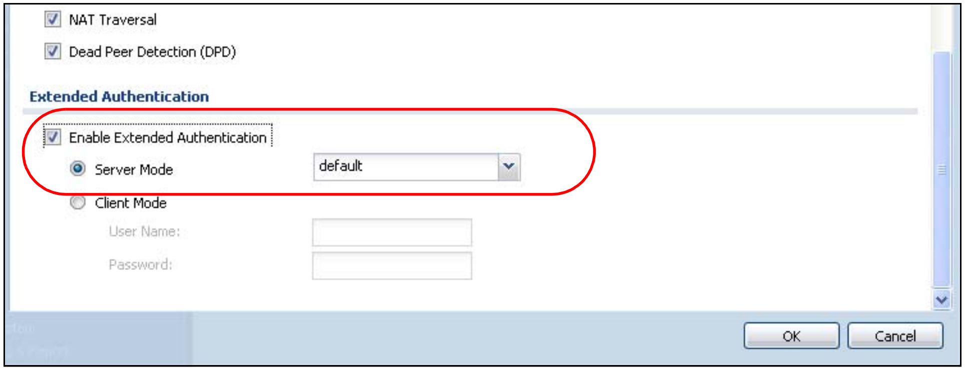
Follow the steps below to specify the authentication method for a VPN connection.

1 Access the **Configuration > VPN > IPSec VPN > VPN Gateway** > **Edit** screen.

2 Click **Show Advance Setting** and select **Enable Extended Authentication**.

3 Select **Server Mode** and select an authentication method object from the drop-down list box.

4 Click **OK** to save the settings.



☑ NAT Traversal

☑ Dead Peer Detection (DPD)

Extended Authentication

☑ Enable Extended Authentication

● Server Mode: default

○ Client Mode

User Name:

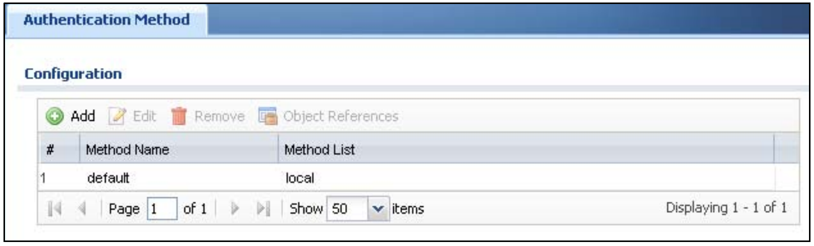
Password:

Figure 427 Example: Using Authentication Method in VPN

49.2 Authentication Method Objects

Click **Configuration > Object > Auth. Method** to display the screen as shown.

Note: You can create up to 16 authentication method objects.



Authentication Method

Configuration

#	Method Name	Method List
1	default	local

Figure 428 Configuration > Object > Auth. Method

The following table describes the labels in this screen.

Table 253 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.
Add icon	Click **Add** to add a new entry. Click **Edit** to edit the settings of an entry. Click **Delete** to remove an entry.

49.2.1 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

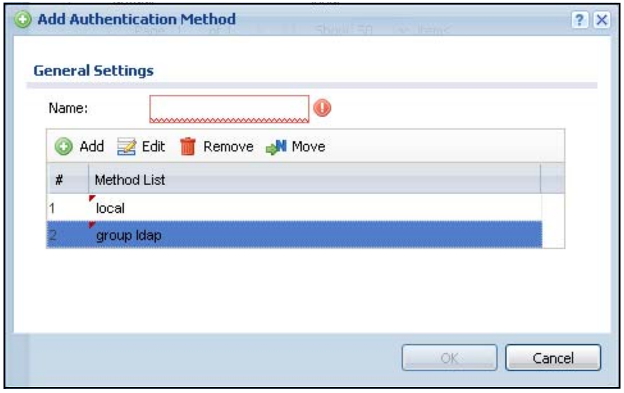
1. Click **Configuration > Object > Auth. Method**.
2. Click **Add**.
3. Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
4. Click **Add** to insert an authentication method in the table.
5. Select a server object from the **Method List** drop-down list box.
6. You can add up to four server objects to the table. The ordering of the **Method List** column is important. The ISG50 authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

   If two accounts with the same username exist on two authentication servers you specify, the ISG50 does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.

   Note: You can NOT select two server objects of the same type.

7. Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 429 Configuration > Object > Auth. Method > Add



#	Method List
1	local
2	group ldap

The following table describes the labels in this screen.

Table 254 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.

Table 254 Configuration > Object > Auth. Method > Add (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Move	To change a method's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed. The ordering of your methods is important as ISG50 authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.
Method List	Select a server object from the drop-down list box. You can create a server object in the **AAA Server** screen (see Chapter 48 on page 631 for more information). The ISG50 authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the ISG50 does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
Add icon	Click **Add** to add a new entry. Click **Edit** to edit the settings of an entry. Click **Delete** to delete an entry.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

50

Certificates

50.1 Overview

The ISG50 can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

50.1.1 What You Can Do in this Chapter

- Use the **My Certificate** screens (see Section 50.2 on page 646 to Section 50.2.3 on page 653) to generate and export self-signed certificates or certification requests and import the ISG50's CA-signed certificates.
- Use the **Trusted Certificates** screens (see Section 50.3 on page 654 to Section 50.3.2 on page 659) to save CA certificates and trusted remote host certificates to the ISG50. The ISG50 trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

50.1.2 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).

2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.

3. Tim uses his private key to sign the message and sends it to Jenny.

4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The ISG50 uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ISG50 does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ISG50 can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The ISG50 only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the ISG50 act as a certification authority and sign its own certificates.

Factory Default Certificate

The ISG50 generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The ISG50 currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ISG50.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

Finding Out More

- See Section 6.7 on page 103 for related information on these screens.
- See Section 50.4 on page 659 for certificate background information.

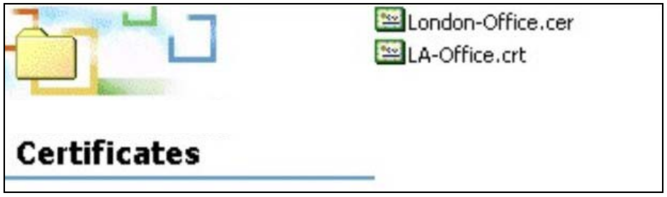
50.1.3 Verifying a Certificate

Before you import a trusted certificate into the ISG50, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

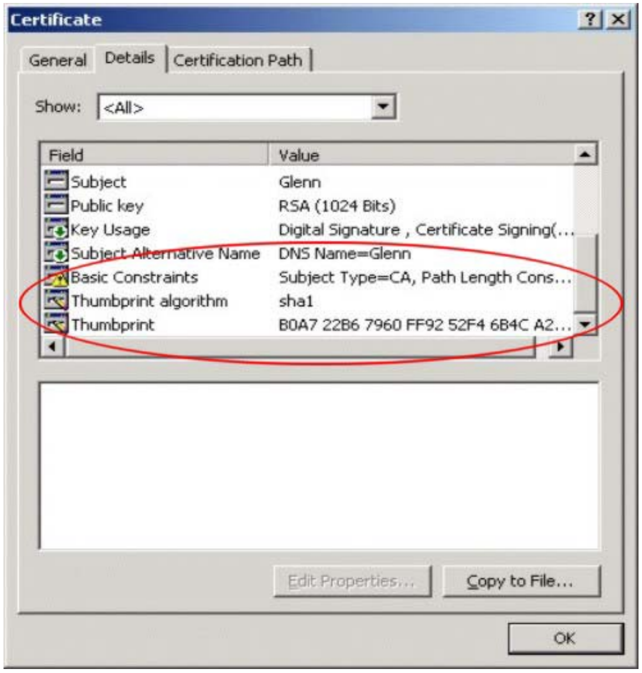
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 430 Remote Host Certificates



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 431 Certificate Details


Certificate
General
Details
Certification Path
Show: <All>
Edit Properties...
Copy to File...
OK

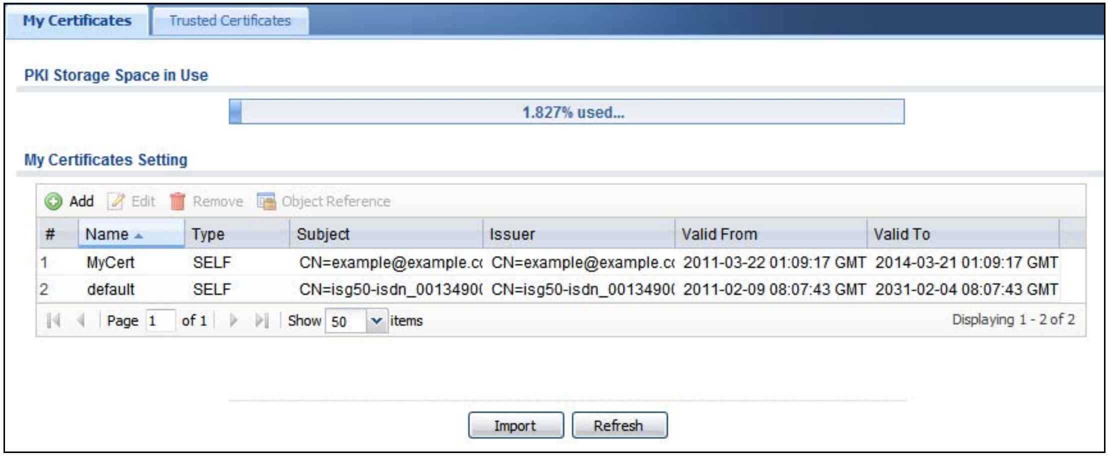
Field	Value
Subject	Glenn
Public key	RSA (1024 Bits)
Key Usage	Digital Signature , Certificate Signing(...
Subject Alternative Name	DNS Name=Glenn
Basic Constraints	Subject Type=CA, Path Length Cons...
Thumbprint algorithm	sha1
Thumbprint	B0A7 22B6 7960 FF92 52F4 6B4C A2...

4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

50.2 The My Certificates Screen

Click **Configuration > Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the ISG50's summary list of certificates and certification requests.

Figure 432 Configuration > Object > Certificate > My Certificates


My Certificates
Trusted Certificates
PKI Storage Space in Use
1.827% used...
My Certificates Setting
Add
Edit
Remove
Object Reference
Page 1 of 1
Show 50 items
Displaying 1 - 2 of 2
Import
Refresh

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	MyCert	SELF	CN=example@example.c(	CN=example@example.c(	2011-03-22 01:09:17 GMT	2014-03-21 01:09:17 GMT
2	default	SELF	CN=isg50-isdn_0013490(	CN=isg50-isdn_0013490(	2011-02-09 08:07:43 GMT	2031-02-04 08:07:43 GMT

The following table describes the labels in this screen.

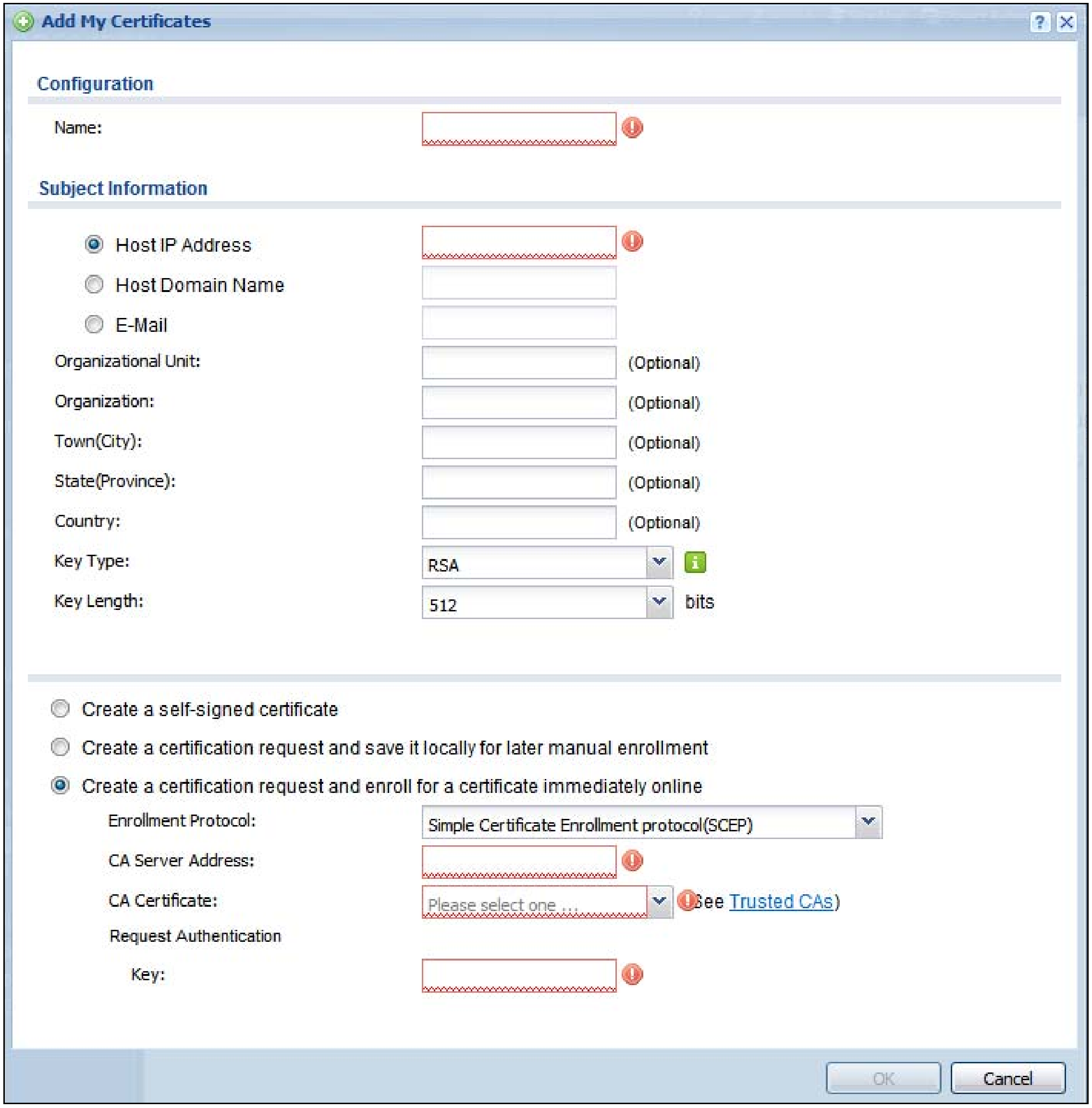
Table 255 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ISG50's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the ISG50 generate a certificate or a certification request.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The ISG50 keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the ISG50's features are configured to use. Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save a certificate to the ISG50.
Refresh	Click **Refresh** to display the current validity status of the certificates.

50.2.1 The My Certificates Add Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the ISG50 create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 433 Configuration > Object > Certificate > My Certificates > Add



Add My Certificates

Configuration

Name:

Subject Information

● Host IP Address

○ Host Domain Name

○ E-Mail

Organizational Unit: (Optional)

Organization: (Optional)

Town(City): (Optional)

State(Province): (Optional)

Country: (Optional)

Key Type: RSA

Key Length: 512 bits

○ Create a self-signed certificate

○ Create a certification request and save it locally for later manual enrollment

● Create a certification request and enroll for a certificate immediately online

Enrollment Protocol: Simple Certificate Enrollment protocol(SCEP)

CA Server Address:

CA Certificate: Please select one ... (See Trusted CAs)

Request Authentication

Key:

The following table describes the labels in this screen.

Table 256 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a **Host IP Address**, **Host Domain Name**, or **E-Mail**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate’s owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State, (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select **RSA** to use the Rivest, Shamir and Adleman public-key algorithm. Select **DSA** to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the ISG50 generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the ISG50 generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 50.2.2 on page 651) and then send it to the certification authority.

Table 256 Configuration > Object > Certificate > My Certificates > Add (continued)

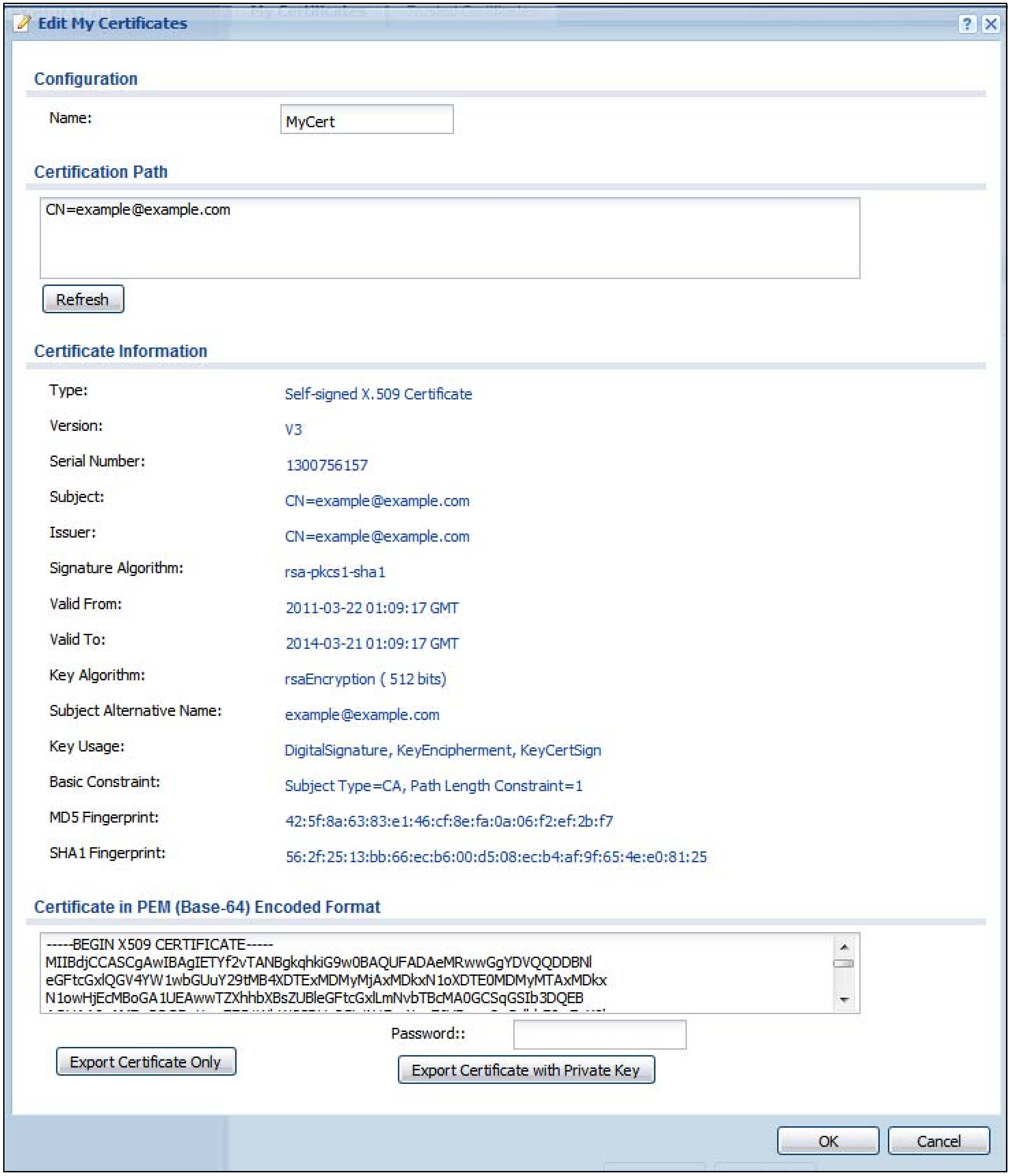
LABEL	DESCRIPTION
Create a certification request and enroll for a certificate immediately online	Select this to have the ISG50 generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server. For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-
CA Certificate	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. Click **Trusted CAs** to go to the **Trusted Certificates** screen where you can view (and manage) the ISG50's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses the CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol. For the reference number, use 0 to 99999999. For the key, use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ISG50 enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ISG50 to enroll a certificate online.

50.2.2 The My Certificates Edit Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 434 Configuration > Object > Certificate > My Certificates > Edit



Edit My Certificates
Configuration
Certification Path
Refresh
Certificate Information
Certificate in PEM (Base-64) Encoded Format
Export Certificate Only
Export Certificate with Private Key
OK
Cancel

Name: MyCert

CN=example@example.com

Type:	Self-signed X.509 Certificate
Version:	V3
Serial Number:	1300756157
Subject:	CN=example@example.com
Issuer:	CN=example@example.com
Signature Algorithm:	rsa-pkcs1-sha1
Valid From:	2011-03-22 01:09:17 GMT
Valid To:	2014-03-21 01:09:17 GMT
Key Algorithm:	rsaEncryption (512 bits)
Subject Alternative Name:	example@example.com
Key Usage:	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint:	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint:	42:5f:8a:63:83:e1:46:cf:8e:fa:0a:06:f2:ef:2b:f7
SHA1 Fingerprint:	56:2f:25:13:bb:66:ec:b6:00:d5:08:ec:b4:af:9f:65:4e:e0:81:25

-----BEGIN X509 CERTIFICATE-----
MIIBdjCCASCgAwIBAgIETYf2vTANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDDBNl
eGFtcGxlQGV4YW1wbGUuY29tMB4XDTExMDMyMjAxMDkxN1oXDTE0MDMyMTAxMDkx
N1owHjEcMBoGA1UEAwwTZXhhbXBsZUBleGFtcGxlLmNvbTBcMA0GCSqGSIb3DQEB

Password::

The following table describes the labels in this screen.

Table 257 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ISG50 does not trust the certificate and displays “Not trusted” in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate’s owner signed the certificate (not a certification authority). “X.509” means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number. “
Serial Number	This field displays the certificate’s identification number given by the certification authority or generated by the ISG50.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. “none” displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ISG50 uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. “none” displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. “none” displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate’s key pair (the ISG50 uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL).

Table 257 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Key Usage	This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate’s message digest that the ISG50 calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate’s message digest that the ISG50 calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority’s web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	This button displays for a certification request. Use this button to save a copy of the request without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate’s password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the ISG50. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

50.2.3 The My Certificates Import Screen

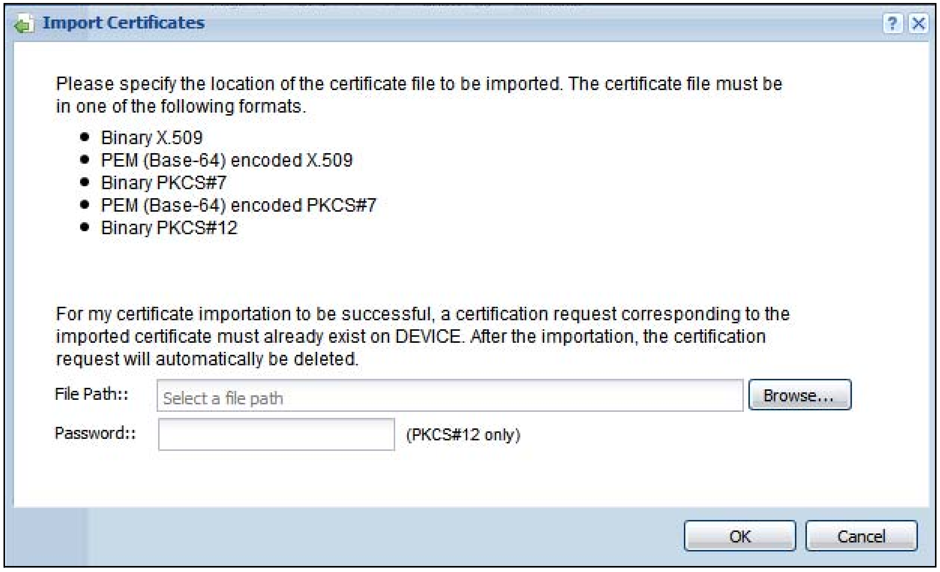
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ISG50.

Note: You can import a certificate that matches a corresponding certification request that was generated by the ISG50. You can also import a certificate in PKCS#12 format, including the certificate’s public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 435 Configuration > Object > Certificate > My Certificates > Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7
- Binary PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on DEVICE. After the importation, the certification request will automatically be deleted.

File Path:: Select a file path

Password:: (PKCS#12 only)

The following table describes the labels in this screen.

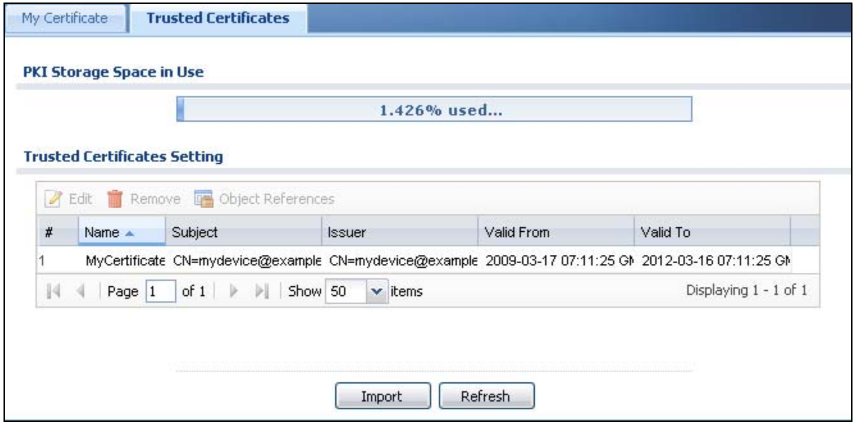
Table 258 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the ISG50.
Browse	Click **Browse** to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the ISG50.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

50.3 The Trusted Certificates Screen

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the ISG50 to accept as trusted. The ISG50 also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 436 Configuration > Object > Certificate > Trusted Certificates



#	Name	Subject	Issuer	Valid From	Valid To
1	MyCertificate	CN=mydevice@example	CN=mydevice@example	2009-03-17 07:11:25 G	2012-03-16 07:11:25 G

The following table describes the labels in this screen.

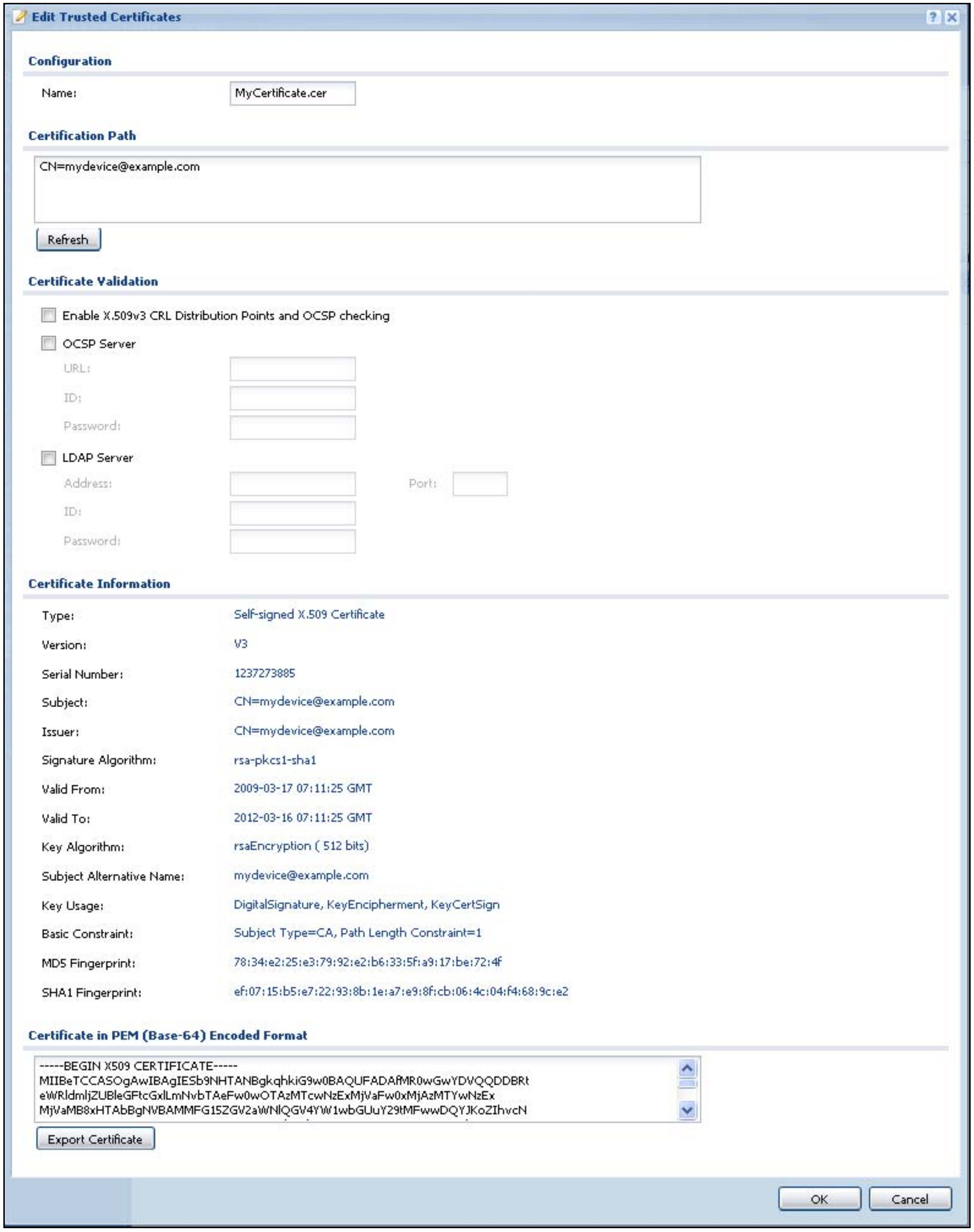
Table 259 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ISG50’s PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The ISG50 keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the ISG50’s features are configured to use. Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ISG50.
Refresh	Click this button to display the current validity status of the certificates.

50.3.1 The Trusted Certificates Edit Screen

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the ISG50 to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 437 Configuration > Object > Certificate > Trusted Certificates > Edit


Edit Trusted Certificates
Configuration
Certification Path
Refresh
Certificate Validation
Certificate Information
Certificate in PEM (Base-64) Encoded Format
Export Certificate
OK
Cancel

Name: MyCertificate.cer

CN=mydevice@example.com

☐ Enable X.509v3 CRL Distribution Points and OCSP checking

☐ OCSP Server

URL:

ID:

Password:

☐ LDAP Server

Address: Port:

ID:

Password:

Type:	Self-signed X.509 Certificate
Version:	V3
Serial Number:	1237273885
Subject:	CN=mydevice@example.com
Issuer:	CN=mydevice@example.com
Signature Algorithm:	rsa-pkcs1-sha1
Valid From:	2009-03-17 07:11:25 GMT
Valid To:	2012-03-16 07:11:25 GMT
Key Algorithm:	rsaEncryption (512 bits)
Subject Alternative Name:	mydevice@example.com
Key Usage:	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint:	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint:	78:34:e2:25:e3:79:92:e2:b6:33:5f:a9:17:be:72:4f
SHA1 Fingerprint:	ef:07:15:b5:e7:22:93:8b:1e:a7:e9:8f:cb:06:4c:04:f4:68:9c:e2

```
-----BEGIN X509 CERTIFICATE-----
MIIBeTCCASOgAwIBAgIESb9NHTANBgkqhkiG9w0BAQUFADAfMR0wGwYDVQQDDBRt
eWRldmljZUBleGFtcGxlLmNvbTAeFw0wOTAzMTcwNzExMjVaFw0xMjAzMTYwNzEx
MjVaMB8xHTAbBgNVBAMMFG15ZGV2aWNlQGV4YW1wbGUuY29tMFwwDQYJKoZIhvcN
```

The following table describes the labels in this screen.

Table 260 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=- characters.
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity’s certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity’s certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity’s own certificate). The ISG50 does not trust the end entity’s certificate and displays “Not trusted” in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to have the ISG50 check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The ISG50 may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The ISG50 may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate’s owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate’s identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 260 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

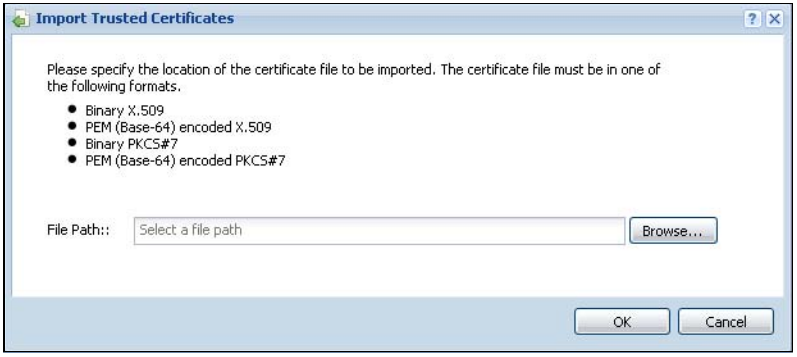
LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ISG50 uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ISG50 calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ISG50 calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the ISG50. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

50.3.2 The Trusted Certificates Import Screen

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the ISG50.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 438 Configuration > Object > Certificate > Trusted Certificates > Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

The following table describes the labels in this screen.

Table 261 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the ISG50.
Browse	Click **Browse** to find the certificate file you want to upload.
OK	Click **OK** to save the certificate on the ISG50.
Cancel	Click **Cancel** to quit and return to the previous screen.

50.4 Certificates Technical Reference

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the ISG50 checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the ISG50 only gets information on the certificates that it needs to verify, not a huge list. When the ISG50 requests certificate status information, the OCSP server returns a “expired”, “current” or “unknown” response.

51

ISP Accounts

51.1 Overview

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. An ISP account is a profile of settings for Internet access using PPPoE or PPTP.

Finding Out More

- See Section 12.4 on page 246 for information about PPPoE/PPTP interfaces.
- See Section 6.7 on page 103 for related information on these screens.

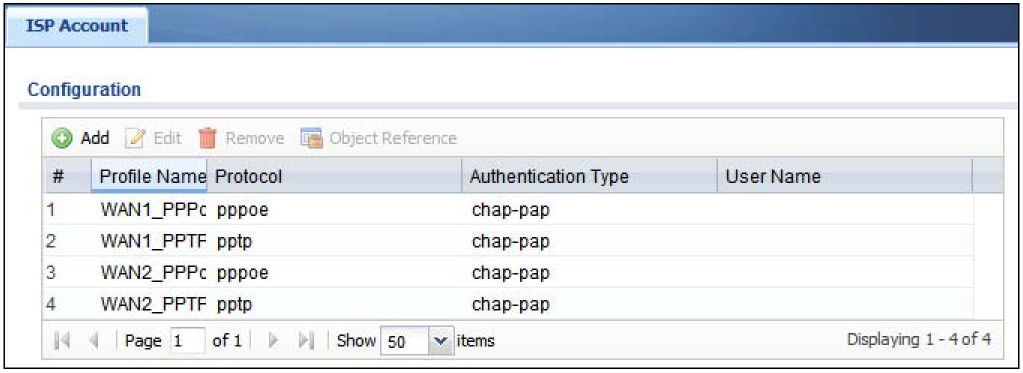
51.1.1 What You Can Do in this Chapter

Use the **Object** > **ISP Account** screens (Section 51.2 on page 661) to create and manage ISP accounts in the ISG50.

51.2 ISP Account Summary

This screen provides a summary of ISP accounts in the ISG50. To access this screen, click **Configuration > Object** > **ISP Account**.

Figure 439 Configuration > Object > ISP Account


ISP Account
Configuration
Add
Edit
Remove
Object Reference
Page 1 of 1
Show 50 items
Displaying 1 - 4 of 4

#	Profile Name	Protocol	Authentication Type	User Name
1	WAN1_PPPc	pppoe	chap-pap	
2	WAN1_PPTF	pptp	chap-pap	
3	WAN2_PPPc	pppoe	chap-pap	
4	WAN2_PPTF	pptp	chap-pap	

The following table describes the labels in this screen. See the ISP Account Add/Edit section below for more information as well.

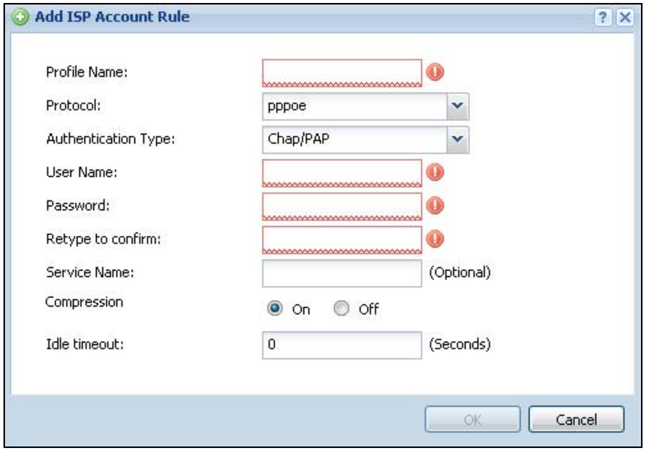
Table 262 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 12.3.2 on page 246 for an example.
#	This field is a sequential value, and it is not associated with a specific entry.
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

51.2.1 ISP Account Add/Edit

The **ISP Account Add** or **Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See Section 51.2 on page 661.) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 440 Configuration > Object > ISP Account > Add



Add ISP Account Rule

Profile Name:

Protocol: pppoe

Authentication Type: Chap/PAP

User Name:

Password:

Retype to confirm:

Service Name: (Optional)

Compression ● On ○ Off

Idle timeout: 0 (Seconds)

The following table describes the labels in this screen.

Table 263 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: **pppoe** - This ISP account uses the PPPoE protocol. **pptp** - This ISP account uses the PPTP protocol.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ISG50 accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ISG50 accepts CHAP only. **PAP** - Your ISG50 accepts PAP only. **MSCHAP** - Your ISG50 accepts MSCHAP only. **MSCHAP-V2** - Your ISG50 accepts MSCHAP-V2 only.
Encryption Method	This field is available if this ISP account uses the **PPTP** protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **nomppe** - This ISP account does not use MPPE. **mppe-40** - This ISP account uses 40-bit MPPE. **mppe-128** - This ISP account uses 128-bit MMPE.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Server IP	If this ISP account uses the PPPoE protocol, this field is not displayed. If this ISP account uses the PPTP protocol, type the IP address of the PPTP server.
Connection ID	This field is available if this ISP account uses the **PPTP** protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select **On** button to turn on stac compression, and select **Off** to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the ISG50 automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.

Table 263 Configuration > Object > ISP Account > Edit (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the ISG50. If there are no errors, the program returns to the **ISP Account** screen. If there are errors, a message box explains the error, and the program stays in the **ISP Account Edit** screen.
Cancel	Click **Cancel** to return to the **ISP Account** screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

52

System

52.1 Overview

Use the system screens to configure general ISG50 settings.

52.1.1 What You Can Do in this Chapter

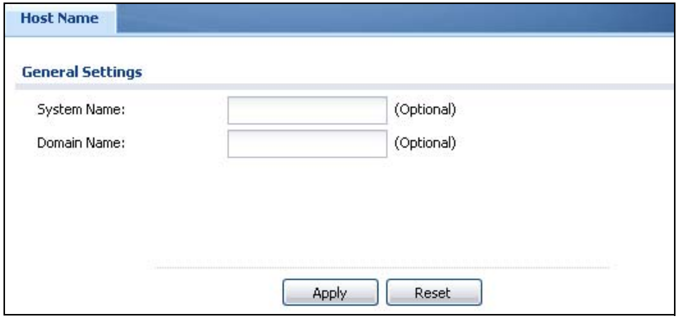
- Use the **System > Host Name** screen (see Section 52.2 on page 666) to configure a unique name for the ISG50 in your network.
- Use the **System > USB Storage** screen (see Section 52.2 on page 666) to configure the settings for the connected USB devices.
- Use the **System > Date/Tim**e screen (see Section 52.4 on page 667) to configure the date and time for the ISG50.
- Use the **System > Console Speed** screen (see Section 52.5 on page 671) to configure the console port speed when you connect to the ISG50 via the console port using a terminal emulation program.
- Use the **System > DNS** screen (see Section 52.6 on page 672) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the **System > WWW** screens (see Section 52.7 on page 678) to configure settings for HTTP or HTTPS access to the ISG50 and how the login and access user screens look.
- Use the **System > SSH** screen (see Section 52.8 on page 693) to configure SSH (Secure SHell) used to securely access the ISG50's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the **System > TELNET** screen (see Section 52.9 on page 698) to configure Telnet to access the ISG50's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the **System > FTP** screen (see Section 52.10 on page 699) to specify from which zones FTP can be used to access the ISG50. You can also specify from which IP addresses the access can come. You can upload and download the ISG50's firmware and configuration files using FTP. Please also see Chapter 55 on page 725 for more information about firmware and configuration files.
- Your ISG50 can act as an SNMP agent, which allows a manager station to manage and monitor the ISG50 through the network. Use the **System > SNMP** screen (see Section 52.11 on page 700) to configure SNMP settings, including from which zones SNMP can be used to access the ISG50. You can also specify from which IP addresses the access can come.
- Use the **System > Language** screen (see Section 52.12 on page 704) to set a language for the ISG50's Web Configurator screens.

Note: See each section for related background information and term definitions.

52.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open the **Host Name** screen.

Figure 441 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 264 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Choose a descriptive name to identify your ISG50 device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

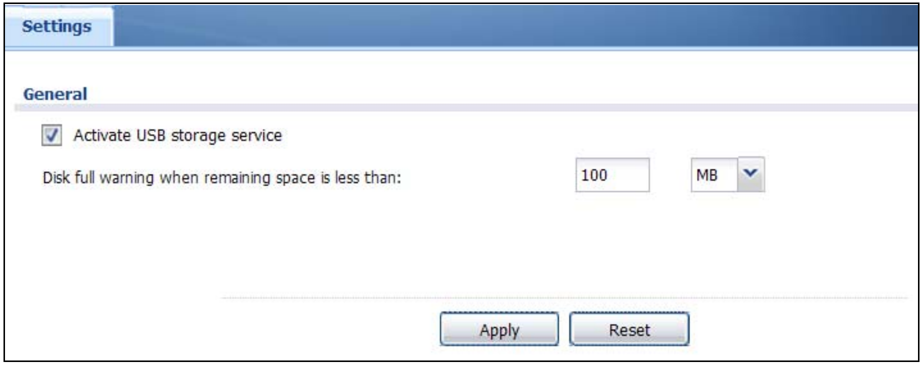
52.3 USB Storage

The ISG50 can use a connected USB device to store the system log and other diagnostic information. Use this screen to turn on this feature and set a disk full warning limit.

Note: Only connect one USB device. Make sure the USB device also uses its external power supply if it has one. It must allow writing (it cannot be read-only) and use the FAT32, EXT2, or EXT3 file system.

Click **Configuration > System > USB Storage** to open the screen as shown next.

Figure 442 Configuration > System > USB Storage



☑ Activate USB storage service

Disk full warning when remaining space is less than: 100 MB

The following table describes the labels in this screen.

Table 265 Configuration > System > USB Storage

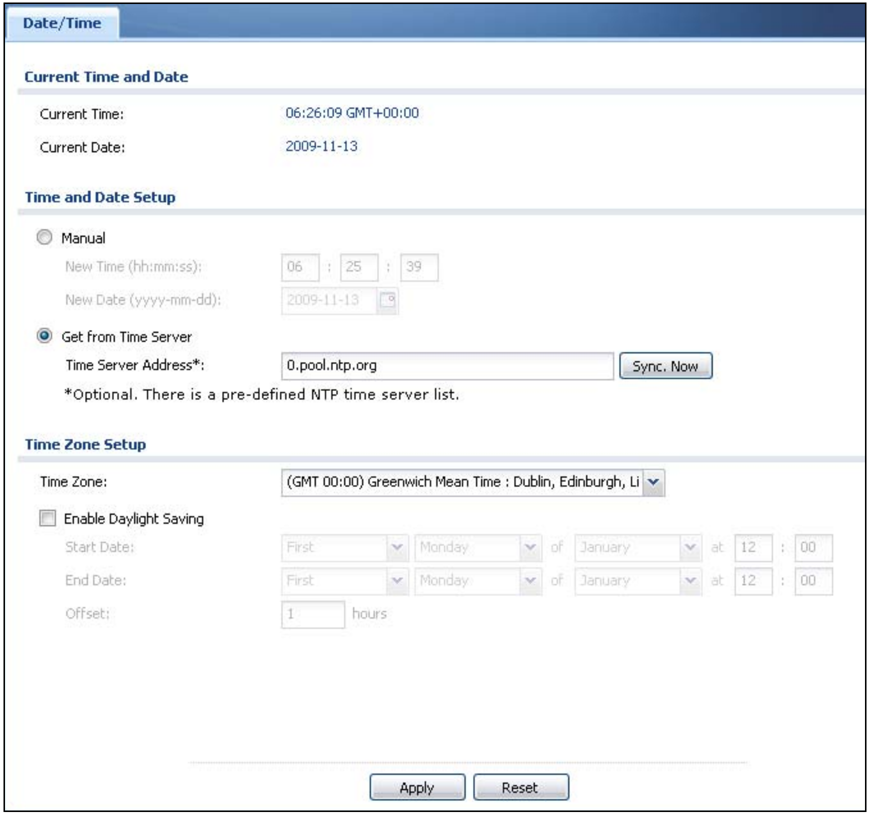
LABEL	DESCRIPTION
Activate USB storage service	Select this if you want to use the connected USB device(s).
Disk full warning when remaining space is less than	Set a number and select a unit (**MB** or **%**) to have the ISG50 send a warning message when the remaining USB storage space is less than the value you set here.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.4 Date and Time

For effective scheduling and logging, the ISG50 system time must be accurate. The ISG50's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your ISG50’s time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the ISG50’s time and date or have the ISG50 get the date and time from a time server.

Figure 443 Configuration > System > Date and Time



Current Time and Date

Current Time: 06:26:09 GMT+00:00
Current Date: 2009-11-13

Time and Date Setup

○ Manual
New Time (hh:mm:ss): 06 : 25 : 39
New Date (yyyy-mm-dd): 2009-11-13
● Get from Time Server
Time Server Address*: 0.pool.ntp.org
*Optional. There is a pre-defined NTP time server list.

Time Zone Setup

Time Zone: (GMT 00:00) Greenwich Mean Time : Dublin, Edinburgh, Li
☐ Enable Daylight Saving
Start Date: First Monday of January at 12 : 00
End Date: First Monday of January at 12 : 00
Offset: 1 hours

The following table describes the labels in this screen.

Table 266 Configuration > System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your ISG50.
Current Date	This field displays the present date of your ISG50.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the ISG50 uses the new setting once you click **Apply**.
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.

Table 266 Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the ISG50 get the time and date from the time server you specify below. The ISG50 requests time and date settings from the time server under the following circumstances. • When the ISG50 starts up. • When you click **Apply** or **Synchronize Now** in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the ISG50 get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.4.1 Pre-defined NTP Time Servers List

When you turn on the ISG50 for the first time, the date and time start at 2003-01-01 00:00:00. The ISG50 then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The ISG50 continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 267 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

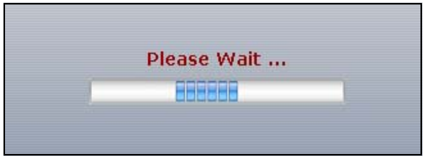
When the ISG50 uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ISG50 goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

52.4.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Please Wait...** screen appears, you may have to wait up to one minute.

Figure 444 Synchronization in Process



Please Wait ...

The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the ISG50 date and time.

1 Click **System > Date/Time**.

2 Select **Manual** under **Time and Date Setup**.

3 Enter the ISG50’s time in the **New Time** field.

4 Enter the ISG50’s date in the **New Date** field.

5 Under **Time Zone Setup**, select your **Time Zone** from the list.

6 As an option you can select the **Enable Daylight Saving** check box to adjust the ISG50 clock for daylight savings.

7 Click **Apply**.

To get the ISG50 date and time from a time server

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

4 As an option you can select the **Enable Daylight Saving** check box to adjust the ISG50 clock for daylight savings.

5 Under **Time and Date Setup**, enter a **Time Server Address** (Table 267 on page 670).

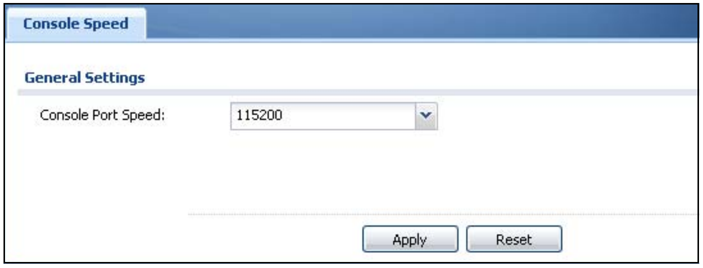
6 Click **Apply**.

52.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the ISG50 via the console port using a terminal emulation program. See Table 2 on page 35 for default console port settings.

Click **Configuration > System > Console Speed** to open the **Console Speed** screen.

Figure 445 Configuration > System > Console Speed



Console Port Speed: 115200

The following table describes the labels in this screen.

Table 268 Configuration > System > Console Speed

LABEL	DESCRIPTION
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your ISG50 supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The **Console Port Speed** applies to a console port connection using terminal emulation software and NOT the **Console** in the ISG50 Web Configurator **Status** screen.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

52.6.1 DNS Server Address Assignment

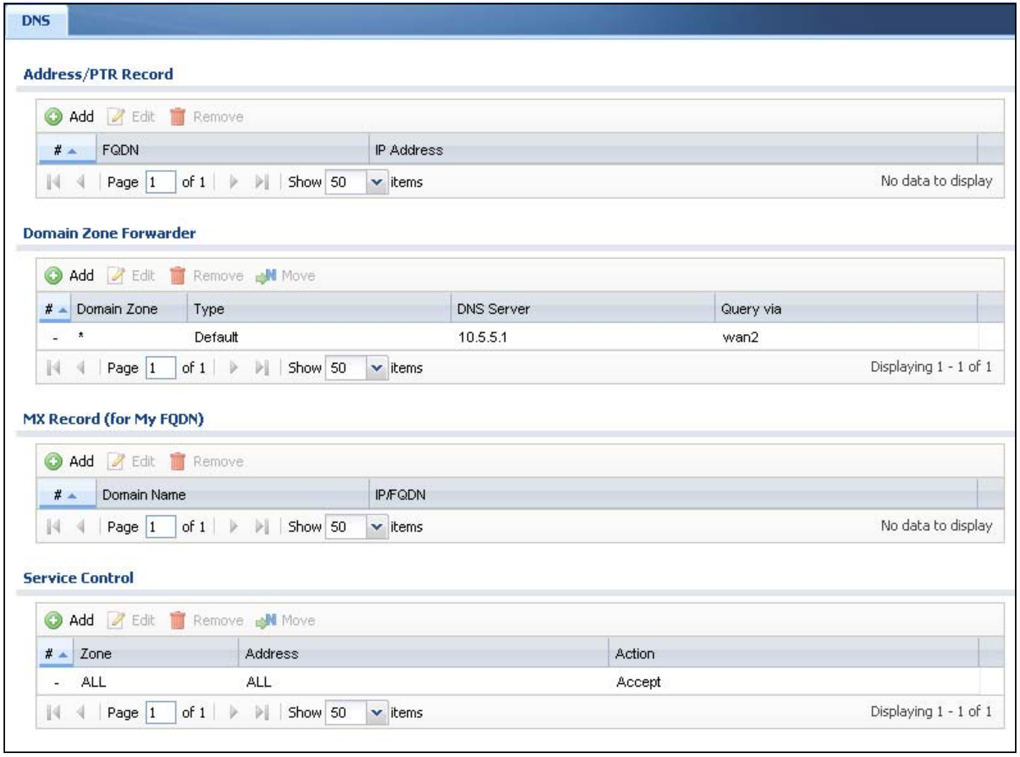
The ISG50 can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the ISG50's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

52.6.2 Configuring the DNS Screen

Click **Configuration > System > DNS** to change your ISG50's DNS settings. Use the **DNS** screen to configure the ISG50 to use a DNS server to resolve domain names for ISG50 system features like VPN, DDNS and the time server. You can also configure the ISG50 to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the ISG50 sends to the specified DHCP client devices.

Figure 446 Configuration > System > DNS



Address/PTR Record

#	FQDN	IP Address

No data to display

Domain Zone Forwarder

#	Domain Zone	Type	DNS Server	Query via
-	*	Default	10.5.5.1	wan2

Displaying 1 - 1 of 1

MX Record (for My FQDN)

#	Domain Name	IP/FQDN

No data to display

Service Control

#	Zone	Address	Action
-	ALL	ALL	Accept

Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 269 Configuration > System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the address/PTR record.
FQDN	This is a host’s fully qualified domain name.
IP Address	This is the IP address of a host.
Domain Zone Forwarder	This specifies a DNS server’s IP address. The ISG50 can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the ISG50 needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry’s position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The ISG50 uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A “*” means all domain zones.
Type	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually (**User-Defined**).
DNS Server	This is the IP address of a DNS server. This field displays **N/A** if you have the ISG50 get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Query Via	This is the interface through which the ISG50 sends DNS queries to the entry’s DNS server. If the ISG50 connects through a VPN tunnel, **tunnel** displays.
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.

Table 269 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
Service Control	This specifies from which computers and zones you can send DNS queries to the ISG50.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry’s position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence. The entry with a hyphen (-) instead of a number is the ISG50’s (non-configurable) default policy. The ISG50 applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ISG50 will not have to use the default policy.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the ISG50 accepts DNS queries from the computer with the IP address specified above through the specified zone (**Accept**) or discards them (**Deny**).

52.6.3 Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com” is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where “mail” is the host, “myZyXEL” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.

The ISG50 allows you to configure address records about the ISG50 itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ISG50 receives a DNS query for an FQDN for which the ISG50 has an address record, the ISG50 can send the IP address in a DNS response without having to query a DNS name server.

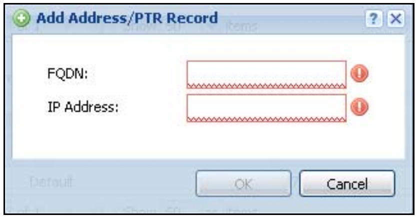
52.6.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

52.6.5 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an address/PTR record.

Figure 447 Configuration > System > DNS > Address/PTR Record Add



The following table describes the labels in this screen.

Table 270 Configuration > System > DNS > Address/PTR Record Add

LABEL	DESCRIPTION
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

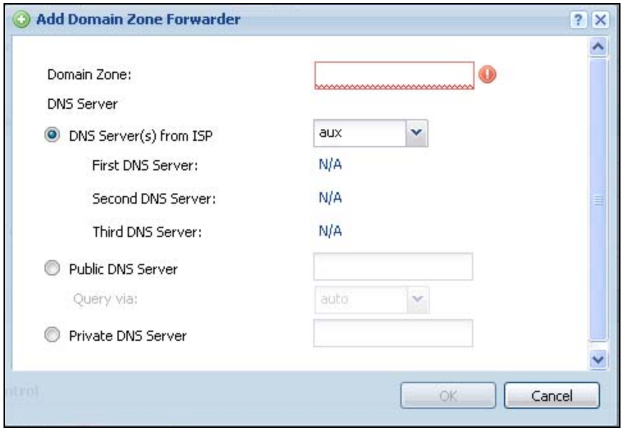
52.6.6 Domain Zone Forwarder

A domain zone forwarder contains a DNS server’s IP address. The ISG50 can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

52.6.7 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

Figure 448 Configuration > System > DNS > Domain Zone Forwarder Add



Domain Zone:
DNS Server
● DNS Server(s) from ISP: aux
First DNS Server: N/A
Second DNS Server: N/A
Third DNS Server: N/A
○ Public DNS Server
Query via: auto
○ Private DNS Server

The following table describes the labels in this screen.

Table 271 Configuration > System > DNS > Domain Zone Forwarder Add

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ISG50 receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select **DNS Server(s) from ISP** if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select **Public DNS Server** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The ISG50 must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the ISG50's local networks. You cannot use 0.0.0.0. Use the **Query via** field to select the interface through which the ISG50 sends DNS queries to a DNS server. Select **Private DNS Server** if you have the IP address of a DNS server to which the ISG50 connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

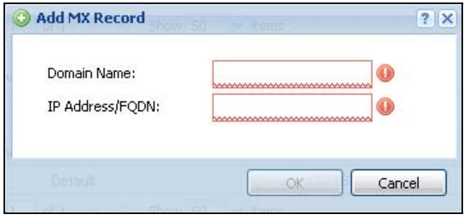
52.6.8 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

52.6.9 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

Figure 449 Configuration > System > DNS > MX Record Add



The following table describes the labels in this screen.

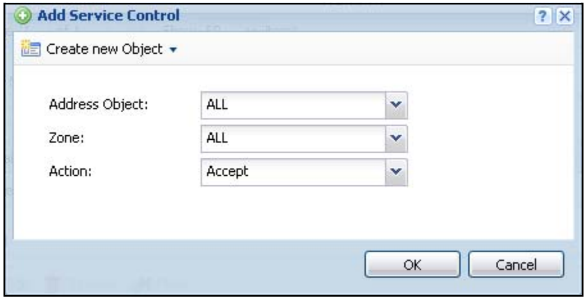
Table 272 Configuration > System > DNS > MX Record Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

52.6.10 Adding a DNS Service Control Rule

Click the **Add** icon in the **Service Control** table to add a service control rule.

Figure 450 Configuration > System > DNS > Service Control Rule Add



Address Object: ALL
Zone: ALL
Action: Accept

The following table describes the labels in this screen.

Table 273 Configuration > System > DNS > Service Control Rule Add

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to send DNS queries to the ISG50. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the ISG50.

Table 273 Configuration > System > DNS > Service Control Rule Add (continued)

LABEL	DESCRIPTION
Zone	Select **ALL** to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the ISG50 is allowed or denied.
Action	Select **Accept** to have the ISG50 allow the DNS queries from the specified computer. Select **Deny** to have the ISG50 reject the DNS queries from the specified computer.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

52.7 WWW Overview

The following figure shows secure and insecure management of the ISG50 coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

- See Section 6.8.1 on page 104 for related information on these screens.

Note: To allow the ISG50 to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ISG50 firewall rule to block that traffic.

- See To-Device Rules on page 354 for more on To-ISG50 firewall rules.
- See Section 7.8 on page 123 for an example of configuring service control to block administrator HTTPS access from all zones except the LAN.

To stop a service from accessing the ISG50, clear **Enable** in the corresponding service screen.

52.7.1 Service Access Limitations

A service cannot be used to access the ISG50 when:

1. You have disabled that service in the corresponding screen.
2. The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the ISG50 disallows the session).
3. The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
4. There is a firewall rule that blocks it.

52.7.2 System Timeout

There is a lease timeout for administrators. The ISG50 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ISG50 for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User/Group** screens.

52.7.3 HTTPS

You can set the ISG50 to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

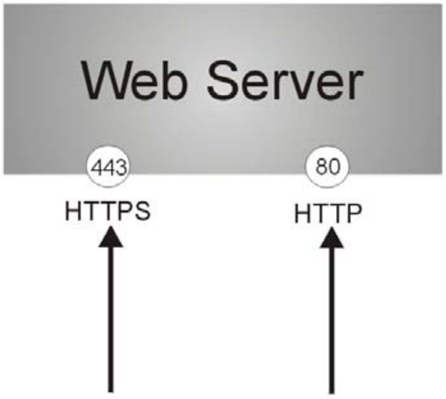
It relies upon certificates, public keys, and private keys (see Chapter 50 on page 643 for more information).

HTTPS on the ISG50 is used so that you can securely access the ISG50 using the Web Configurator. The SSL protocol specifies that the HTTPS server (the ISG50) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the ISG50), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the ISG50 a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ISG50.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ISG50's web server.
2. HTTP connection requests from a web browser go to port 80 (by default) on the ISG50's web server.

Figure 451 HTTP/HTTPS Implementation



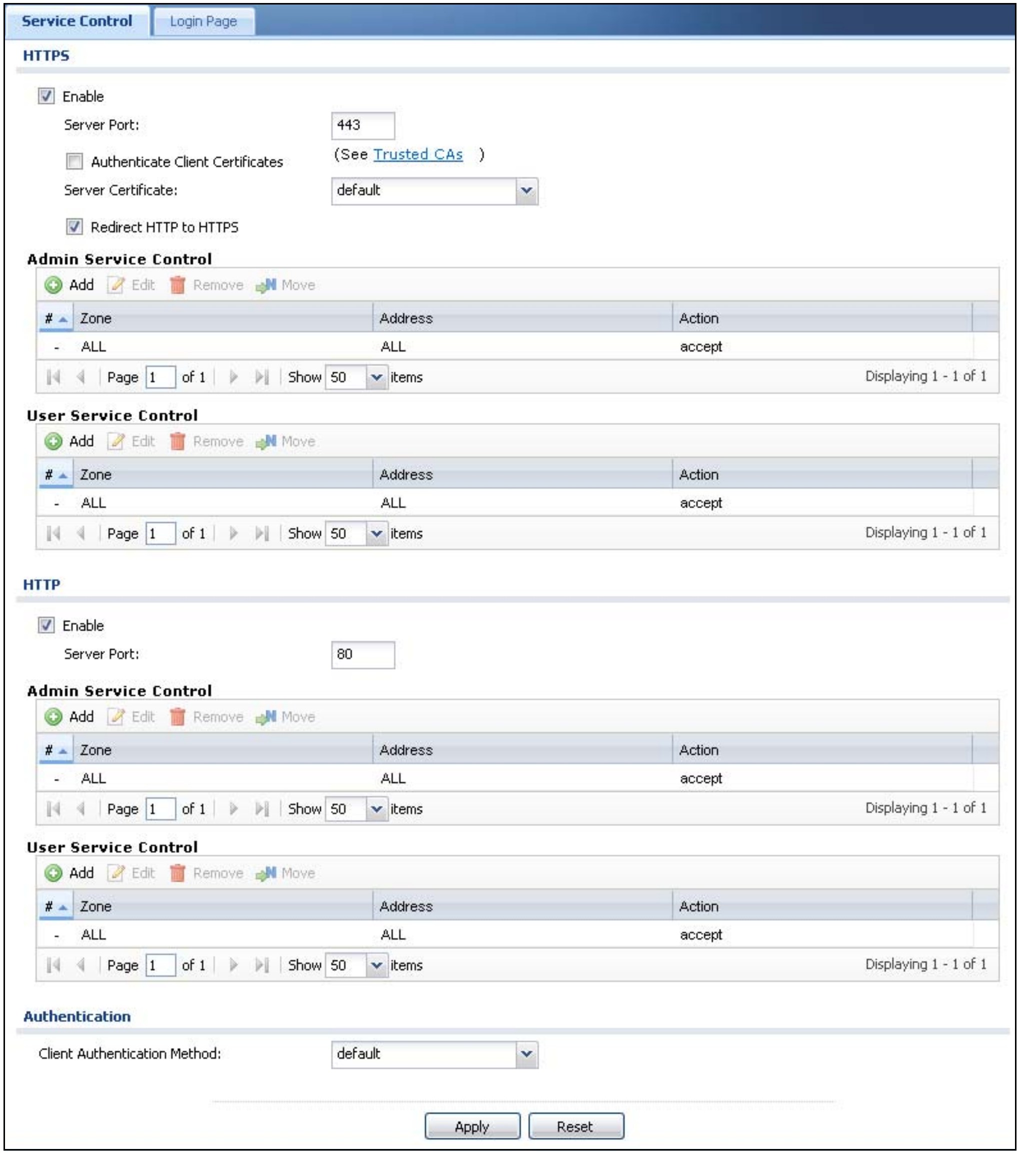
Note: If you disable **HTTP** in the **WWW** screen, then the ISG50 blocks all HTTP connection attempts.

52.7.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify from which zones you can access the ISG50 using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Note: **Admin Service Control** deals with management access (to the Web Configurator). **User Service Control** deals with user access to the ISG50.

Figure 452 Configuration > System > WWW > Service Control



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action
-	ALL	ALL	accept

User Service Control

#	Zone	Address	Action
-	ALL	ALL	accept

HTTP

☑ Enable

Server Port: 80

Admin Service Control

#	Zone	Address	Action
-	ALL	ALL	accept

User Service Control

#	Zone	Address	Action
-	ALL	ALL	accept

Authentication

Client Authentication Method: default

The following table describes the labels in this screen.

Table 274 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ISG50 Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the ISG50, for example 8443, then you must notify people who need to access the ISG50 Web Configurator to use "https://ISG50 IP Address:**8443**" as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ISG50 by sending the ISG50 a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ISG50 (see Section 52.7.7.4 on page 688 on importing certificates for details).
Server Certificate	Select a certificate the HTTPS server (the ISG50) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTPS to manage the ISG50 (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the ISG50. **User Service Control** specifies from which zones a user can use HTTPS to log into the ISG50. You can also specify the IP addresses from which the users can access the ISG50.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ISG50's (non-configurable) default policy. The ISG50 applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ISG50 will not have to use the default policy.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ISG50 zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
HTTP	

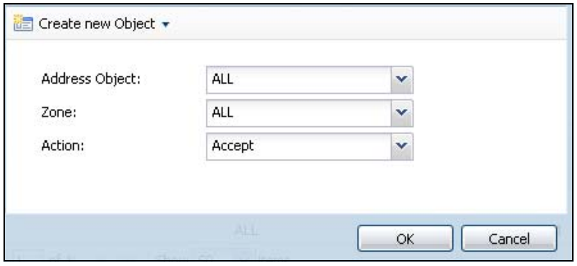
Table 274 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ISG50 Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the ISG50.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTP to manage the ISG50 (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the ISG50. **User Service Control** specifies from which zones a user can use HTTP to log into the ISG50. You can also specify the IP addresses from which the users can access the ISG50.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ISG50's (non-configurable) default policy. The ISG50 applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ISG50 will not have to use the default policy.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ISG50 zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the **Auth. method** screen.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.7.5 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW**, **SSH**, **Telnet**, **FTP** or **SNMP** screen to add a service control rule.

Figure 453 Configuration > System > Service Control Rule > Edit



Address Object: ALL
Zone: ALL
Action: Accept

The following table describes the labels in this screen.

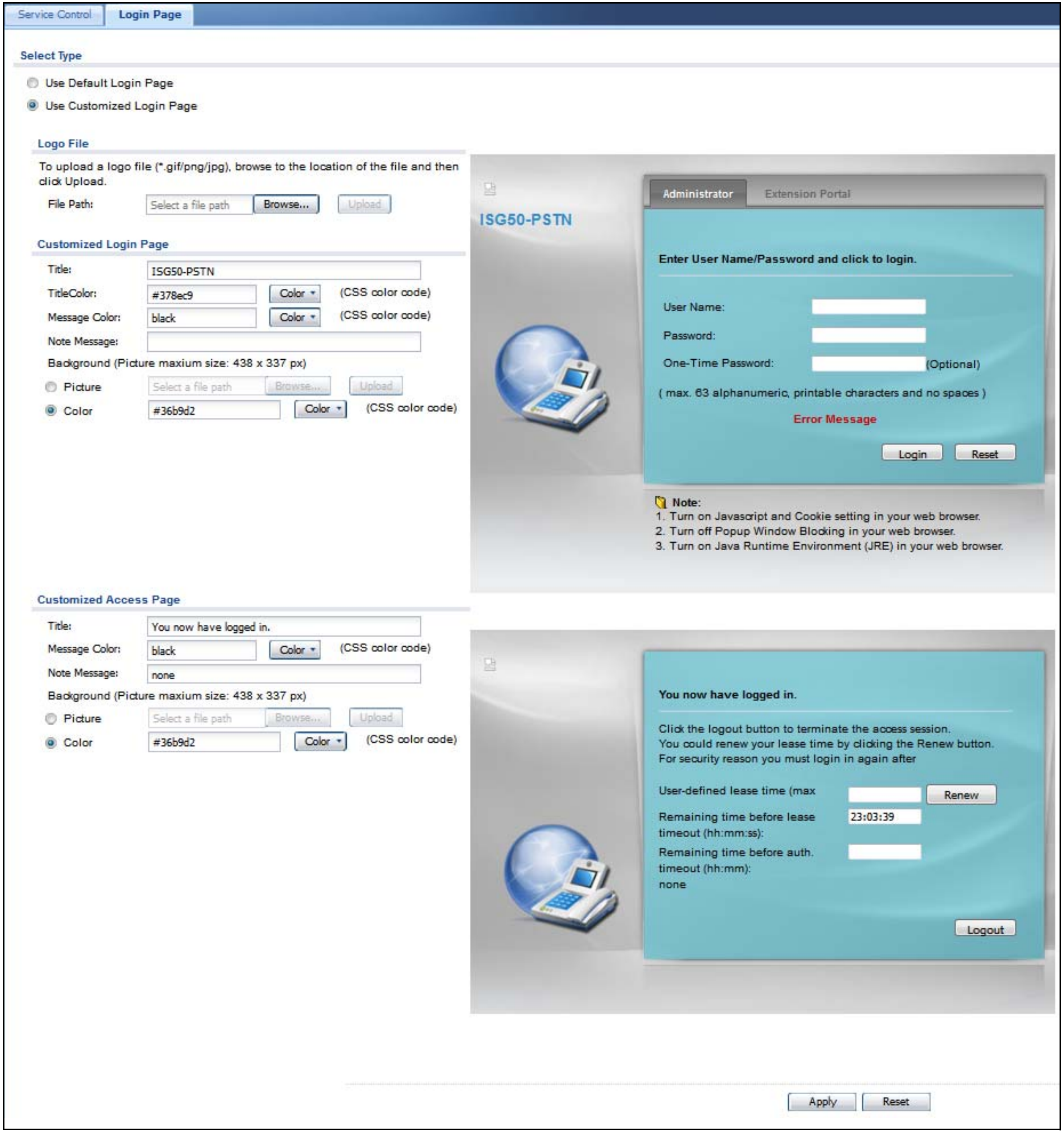
Table 275 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the ISG50 using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the ISG50 using this service.
Zone	Select **ALL** to allow or prevent any ISG50 zones from being accessed using this service. Select a predefined ISG50 zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the ISG50 from the specified computers. Select **Deny** to block the user's access to the ISG50 from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

52.7.6 Customizing the WWW Login Page

Click **Configuration > System > WWW > Login Page** to open the **Login Page** screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See Chapter 44 on page 599 for more on access user accounts.

Figure 454 Configuration > System > WWW > Login Page



Select Type

○ Use Default Login Page

● Use Customized Login Page

Logo File

To upload a logo file (*.gif/png/jpg), browse to the location of the file and then click Upload.

File Path: Select a file path

Customized Login Page

Title: ISG50-PSTN

TitleColor: #378ec9 (CSS color code)

Message Color: black (CSS color code)

Note Message:

Background (Picture maxium size: 438 x 337 px)

○ Picture Select a file path

● Color #36b9d2 (CSS color code)

ISG50-PSTN

Enter User Name/Password and click to login.

User Name:

Password:

One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Error Message

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

Customized Access Page

Title: You now have logged in.

Message Color: black (CSS color code)

Note Message: none

Background (Picture maxium size: 438 x 337 px)

○ Picture Select a file path

● Color #36b9d2 (CSS color code)

You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after

User-defined lease time (max

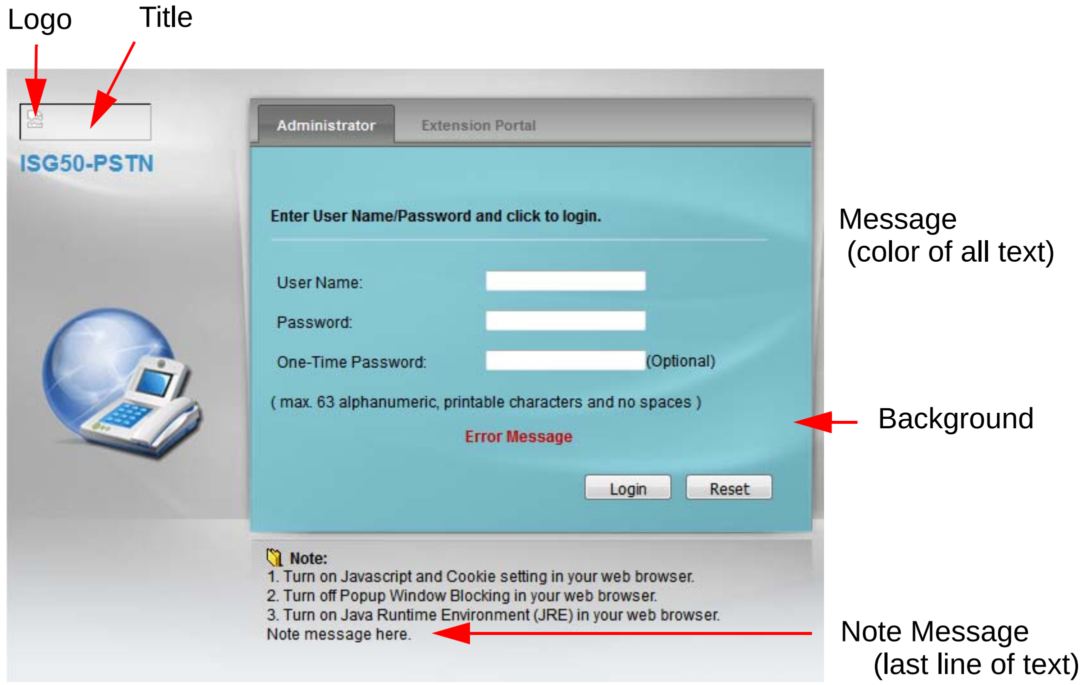
Remaining time before lease timeout (hh:mm:ss): 23:03:39

Remaining time before auth. timeout (hh:mm):

none

The following figures identify the parts you can customize in the login and access pages.

Figure 455 Login Page Customization


Logo
Title
ISG50-PSTN
Administrator
Extension Portal
Message
(color of all text)
Background
Login
Reset
Note Message
(last line of text)

Enter User Name/Password and click to login.

User Name:

Password:

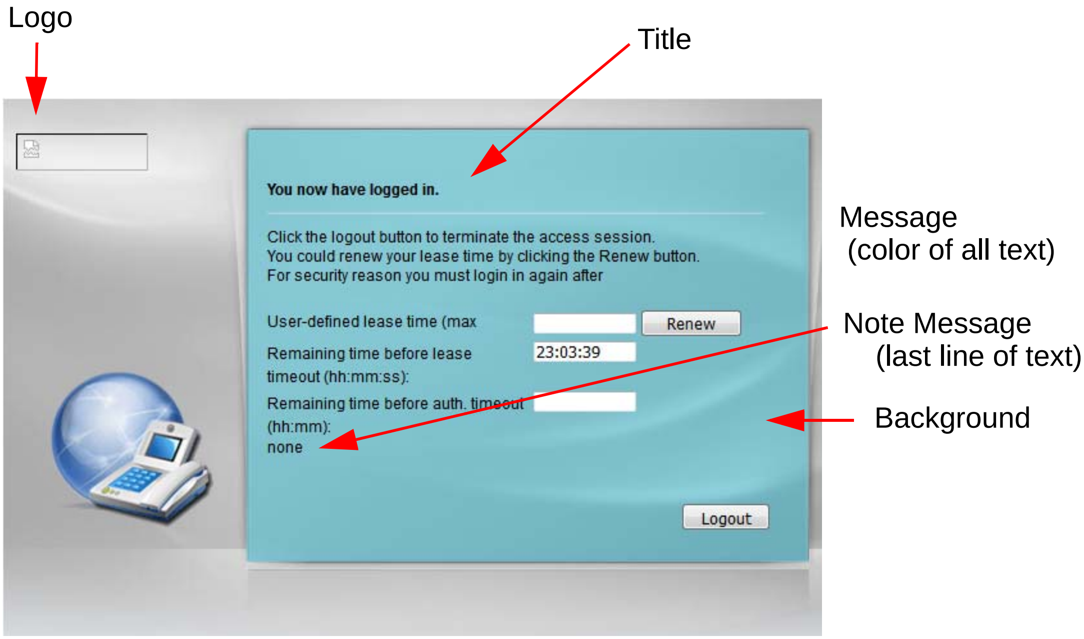
One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Error Message

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
Note message here.

Figure 456 Access Page Customization


Logo
Title
Message
(color of all text)
Note Message
(last line of text)
Background
Renew
Logout

You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after

User-defined lease time (max

Remaining time before lease timeout (hh:mm:ss): 23:03:39

Remaining time before auth. timeout (hh:mm):

none

You can specify colors in one of the following ways:

- Click **Color** to display a screen of web-safe colors from which to choose.
- Enter the name of the desired color.

- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.
- Enter "rgb" followed by red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.

Your desired color should display in the preview screen on the right after you click in another field, click **Apply**, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels in the screen.

Table 276 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Select Type	Select whether the Web Configurator uses the default login screen or one that you customize in the rest of this screen.
Logo File	You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. Click **Upload** to transfer the specified graphic file from your computer to the ISG50.
Customized Login Page	Use this section to set how the Web Configurator login screen looks.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Title Color	Specify the color of the screen's title text.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display at the bottom of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the screen background looks. To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select **Color** and specify the color.
Customized Access Page	Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the screen background looks. To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select **Color** and specify the color.

Table 276 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.7.7 HTTPS Example

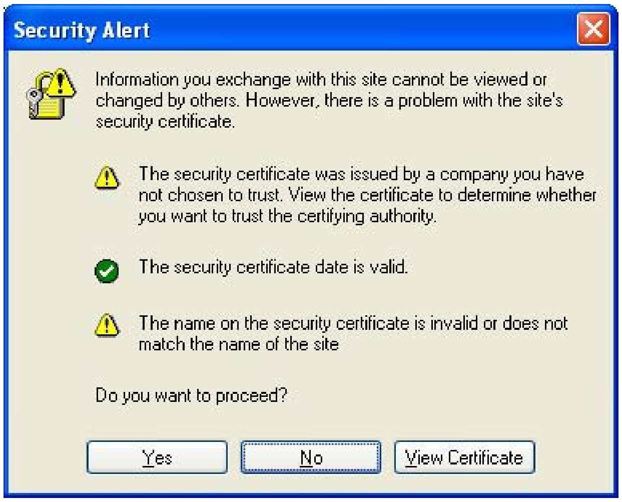
If you haven't changed the default HTTPS port on the ISG50, then in your browser enter "https://ISG50 IP Address/" as the web site address where "ISG50 IP Address" is the IP address or domain name of the ISG50 you wish to access.

52.7.7.1 Internet Explorer Warning Messages

When you attempt to access the ISG50 HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ISG50.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the Web Configurator login screen; if you select **No**, then Web Configurator access is blocked.

Figure 457 Security Alert Dialog Box (Internet Explorer)



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

52.7.7.2 Avoiding Browser Warning Messages

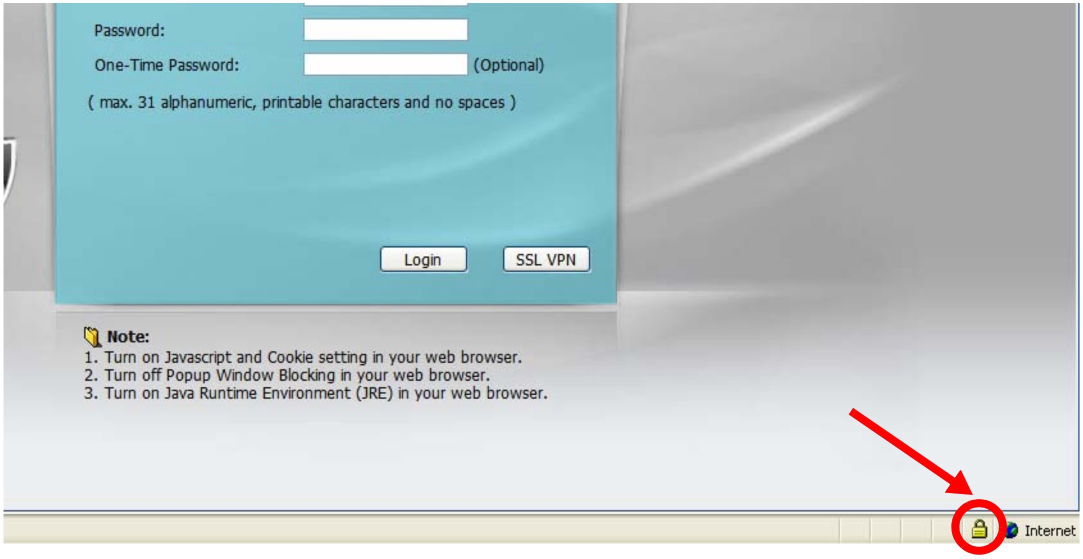
Here are the main reasons your browser displays warnings about the ISG50's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the ISG50's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ISG50's factory default certificate is the ISG50 itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix C on page 831 for details.

52.7.7.3 Login Screen

After you accept the certificate, the ISG50 login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 458 Login Screen (Internet Explorer)


Password:
One-Time Password:
(Optional)
Login
SSL VPN
Internet

(max. 31 alphanumeric, printable characters and no spaces)

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

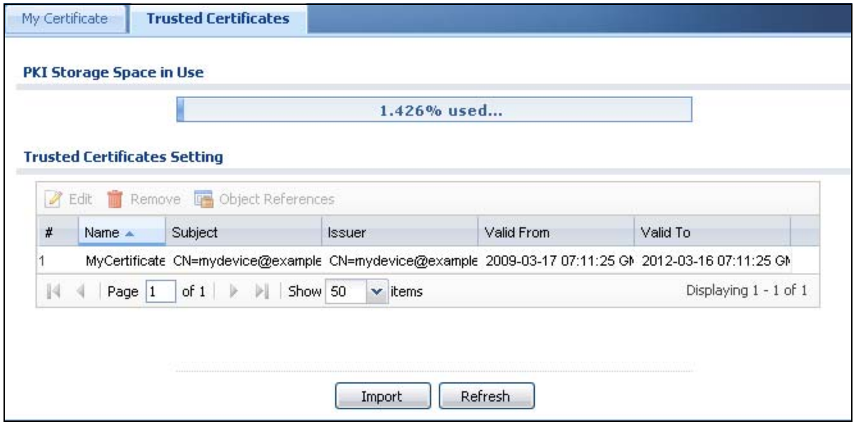
52.7.7.4 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ISG50.

You must have imported at least one trusted CA to the ISG50 in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ISG50 (see the ISG50's **Trusted CA** Web Configurator screen).

Figure 459 ISG50 Trusted CA Screen


My Certificate
Trusted Certificates
PKI Storage Space in Use
1.426% used...
Trusted Certificates Setting
Edit
Remove
Object References
Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1
Import
Refresh

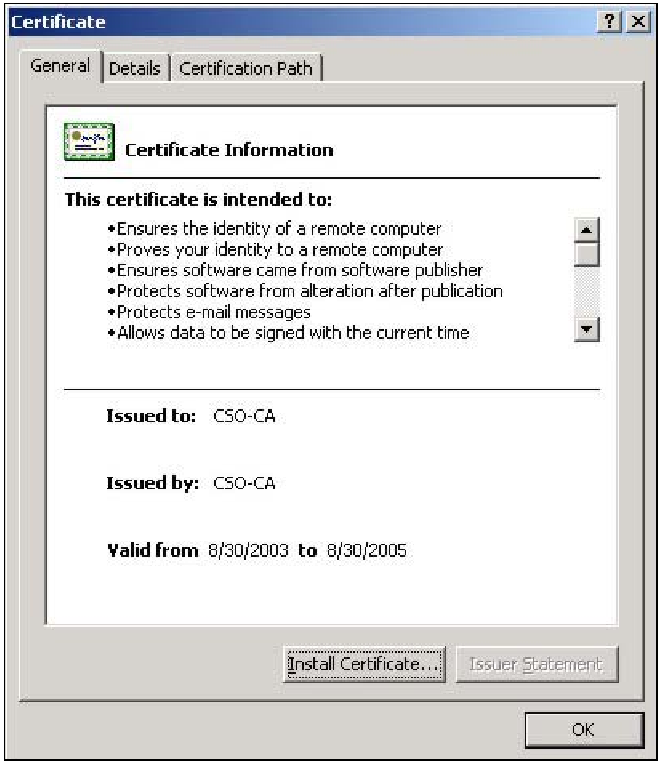
#	Name	Subject	Issuer	Valid From	Valid To
1	MyCertificate	CN=mydevice@example	CN=mydevice@example	2009-03-17 07:11:25 GM	2012-03-16 07:11:25 GM

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

52.7.7.4.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 460 CA Certificate Example



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: CSO-CA

Issued by: CSO-CA

Valid from 8/30/2003 **to** 8/30/2005

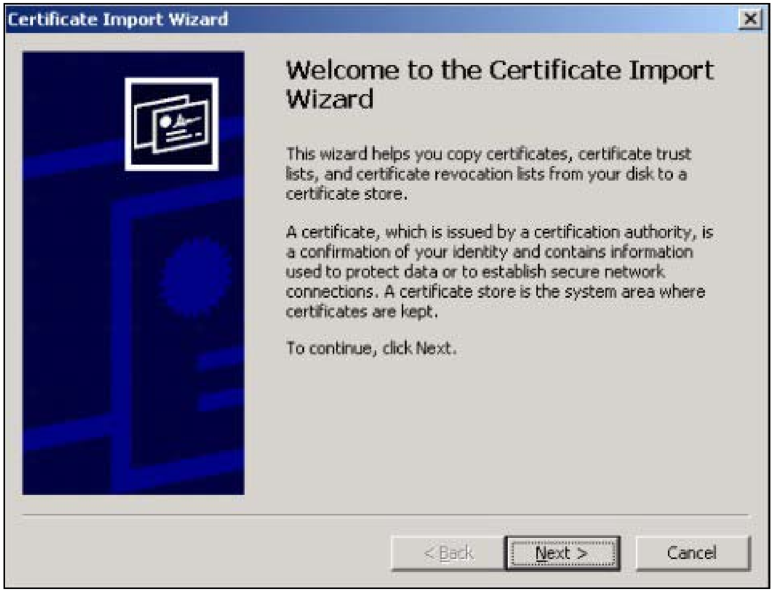
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

52.7.7.4.2 Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

Figure 461 Personal Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

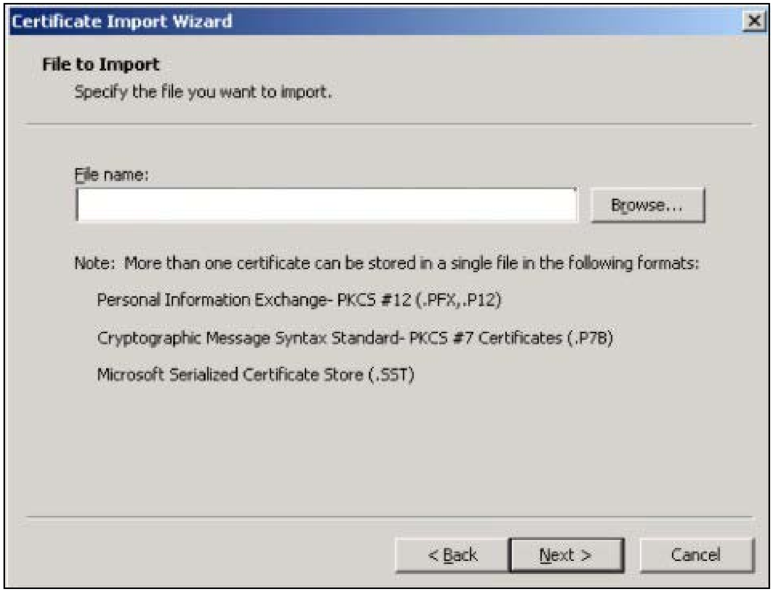
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 462 Personal Certificate Import Wizard 2



Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

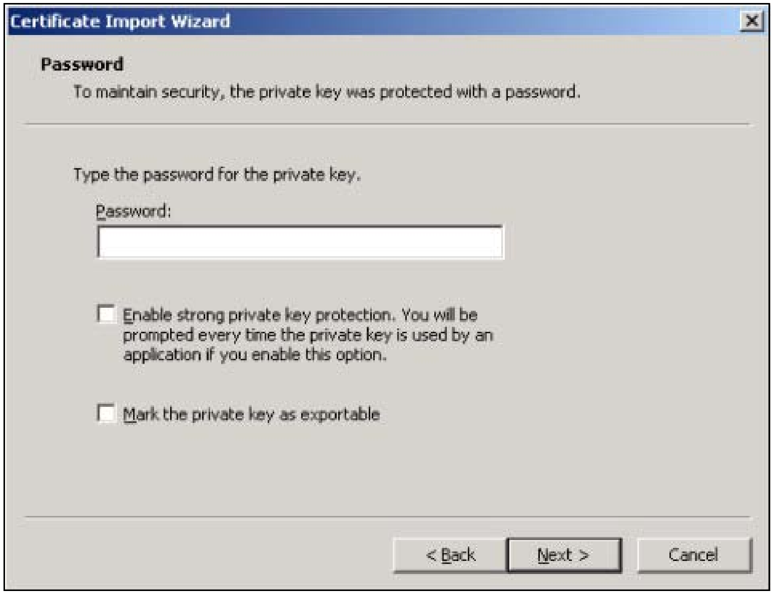
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

Figure 463 Personal Certificate Import Wizard 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

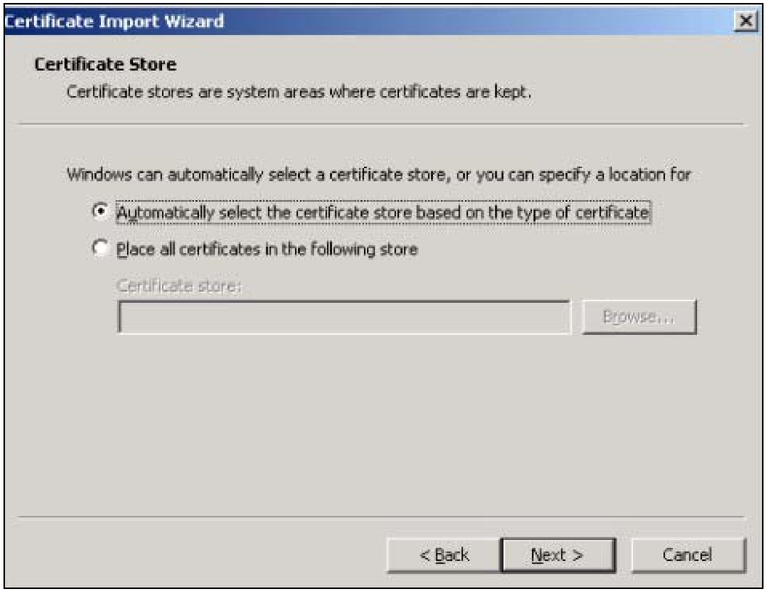
Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark the private key as exportable

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 464 Personal Certificate Import Wizard 4



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

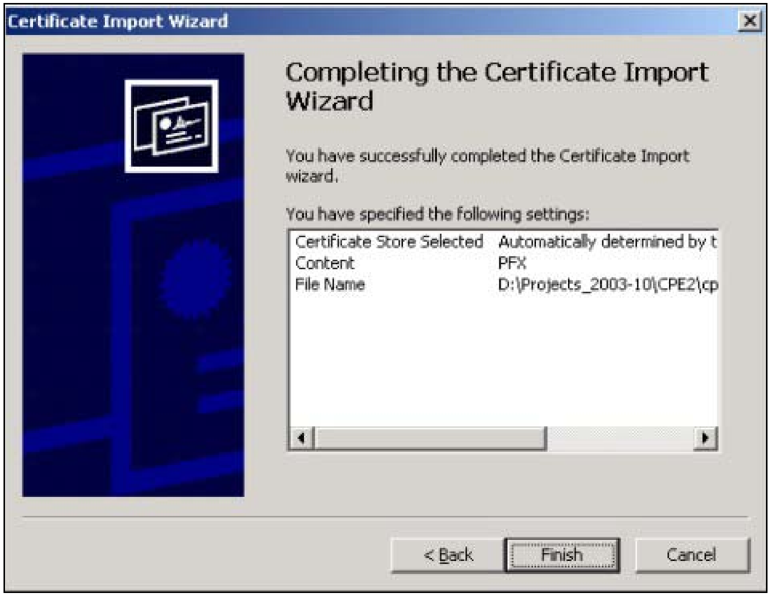
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the wizard and begin the import process.

Figure 465 Personal Certificate Import Wizard 5



Certificate Import Wizard

Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

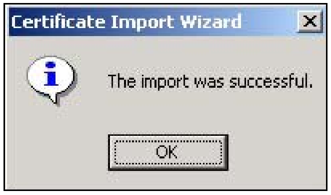
You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	D:\Projects_2003-10\CPE2\cp

< Back
Finish
Cancel

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 466 Personal Certificate Import Wizard 6



Certificate Import Wizard

The import was successful.

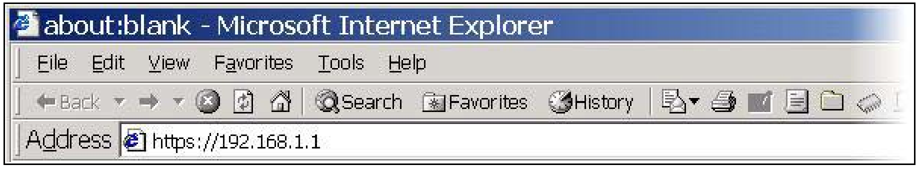
OK

52.7.7.5 Using a Certificate When Accessing the ISG50 Example

Use the following procedure to access the ISG50 via HTTPS.

1 Enter ‘https://ISG50 IP Address/ in your browser’s web address field.

Figure 467 Access the ISG50 Via HTTPS

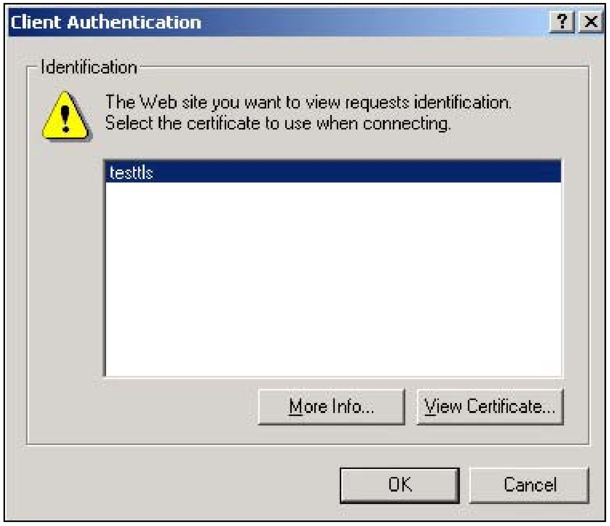


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address

https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the ISG50, the following screen asks you to select a personal certificate to send to the ISG50. This screen displays even if you only have a single certificate as in the example.

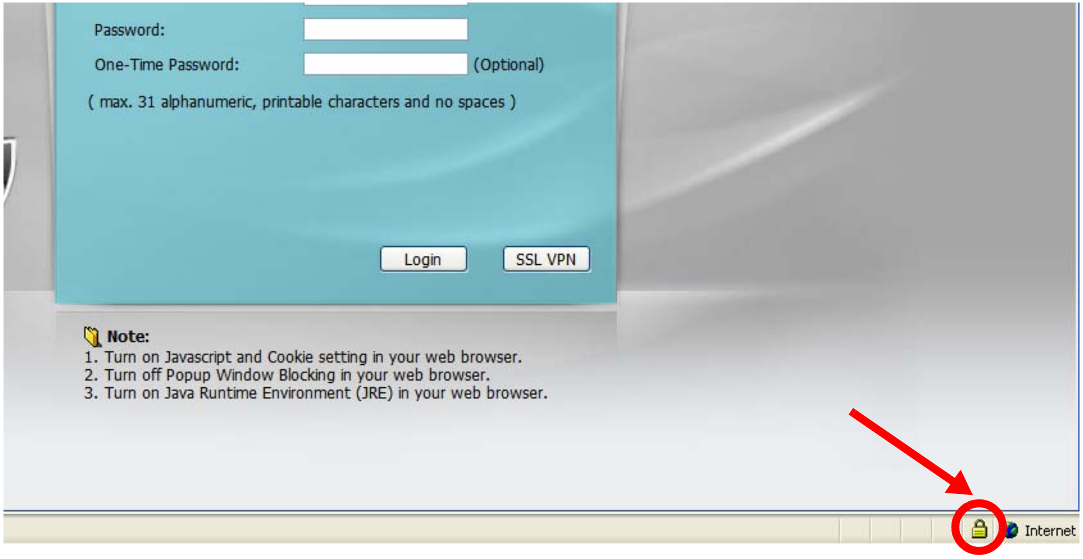
Figure 468 SSL Client Authentication


Client Authentication
Identification
testtls
More Info...
View Certificate...
OK
Cancel

The Web site you want to view requests identification. Select the certificate to use when connecting.

3 You next see the Web Configurator login screen.

Figure 469 Secure Web Configurator Login Screen


Password:
One-Time Password:
(Optional)
Login
SSL VPN
Internet

(max. 31 alphanumeric, printable characters and no spaces)

Note:

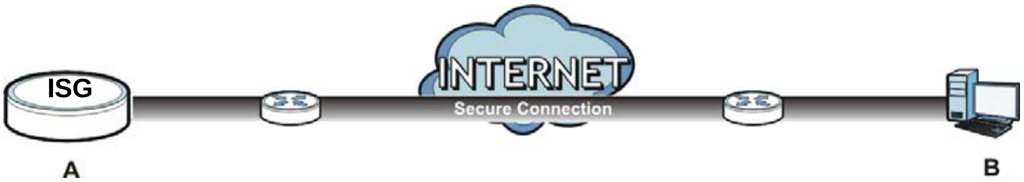
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

52.8 SSH

You can use SSH (Secure SHell) to securely access the ISG50's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the ISG50 for a management session.

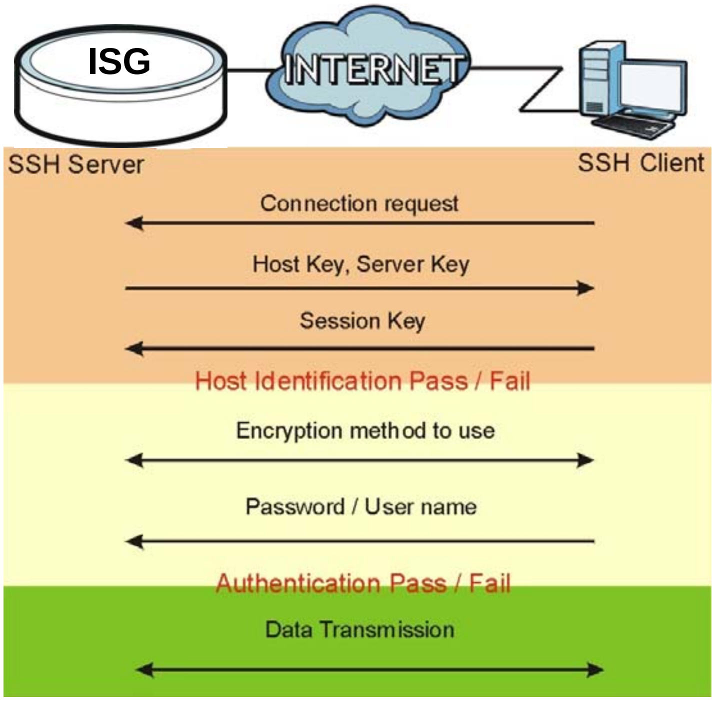
Figure 470 SSH Communication Over the WAN Example


ISG
INTERNET
Secure Connection
A
B

52.8.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 471 How SSH v1 Works Example


ISG
INTERNET
SSH Server
SSH Client
Connection request
Host Key, Server Key
Session Key
Host Identification Pass / Fail
Encryption method to use
Password / User name
Authentication Pass / Fail
Data Transmission

1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

52.8.2 SSH Implementation on the ISG50

Your ISG50 supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the ISG50 for management using port 22 (by default).

52.8.3 Requirements for Using SSH

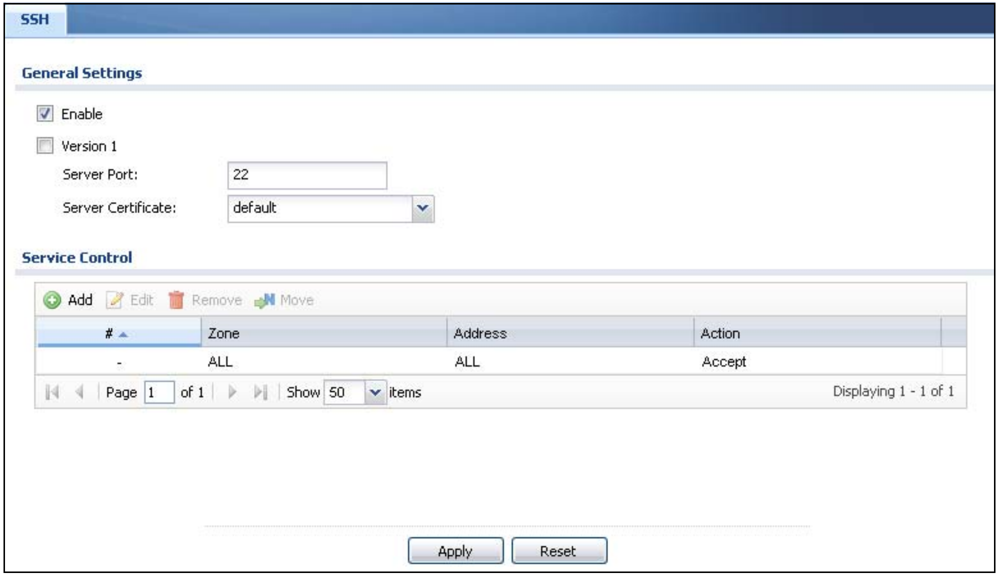
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ISG50 over SSH.

52.8.4 Configuring SSH

Click **Configuration > System > SSH** to change your ISG50's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the ISG50. You can also specify from which IP addresses the access can come.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 472 Configuration > System > SSH



☑ Enable

☐ Version 1

Server Port: 22

Server Certificate: default

#	Zone	Address	Action
-	ALL	ALL	Accept

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 277 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ISG50 CLI using this service.
Version 1	Select the check box to have the ISG50 use both SSH version 1 and version 2 protocols. If you clear the check box, the ISG50 uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ISG50 for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 50 on page 643 for details).
Service Control	This specifies from which computers you can access which ISG50 zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 275 on page 683 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ISG50 zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.8.5 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ISG50. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

52.8.5.1 Example 1: Microsoft Windows

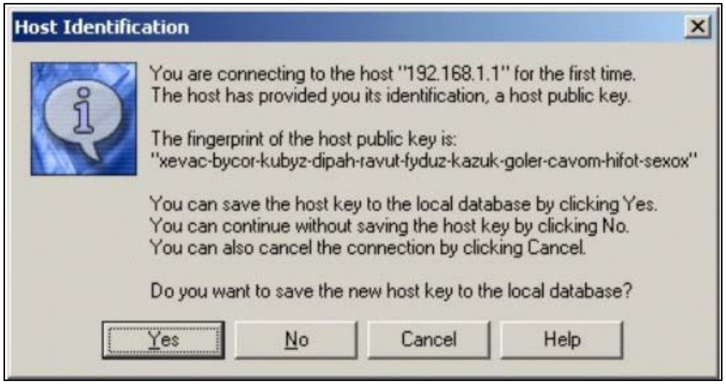
This section describes how to access the ISG50 using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number) for the ISG50.

2. Configure the SSH client to accept connection using SSH version 1.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 473 SSH Example 1: Store Host Key



You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.

The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"

You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.

Do you want to save the new host key to the local database?

Enter the password to log in to the ISG50. The CLI screen displays next.

52.8.5.2 Example 2: Linux

This section describes how to access the ISG50 using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the ISG50.

Enter “`telnet 192.168.1.1 22`” at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ISG50 (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the ISG50.

Figure 474 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter “`ssh –1 192.168.1.1`”. This command forces your computer to connect to the ISG50 using SSH version 1. If this is the first time you are connecting to the ISG50 using SSH, a message displays prompting you to save the host information of the ISG50. Type “yes” and press [ENTER].

Then enter the password to log in to the ISG50.

Figure 475 SSH Example 2: Log in

```
$ ssh –1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI screen displays next.

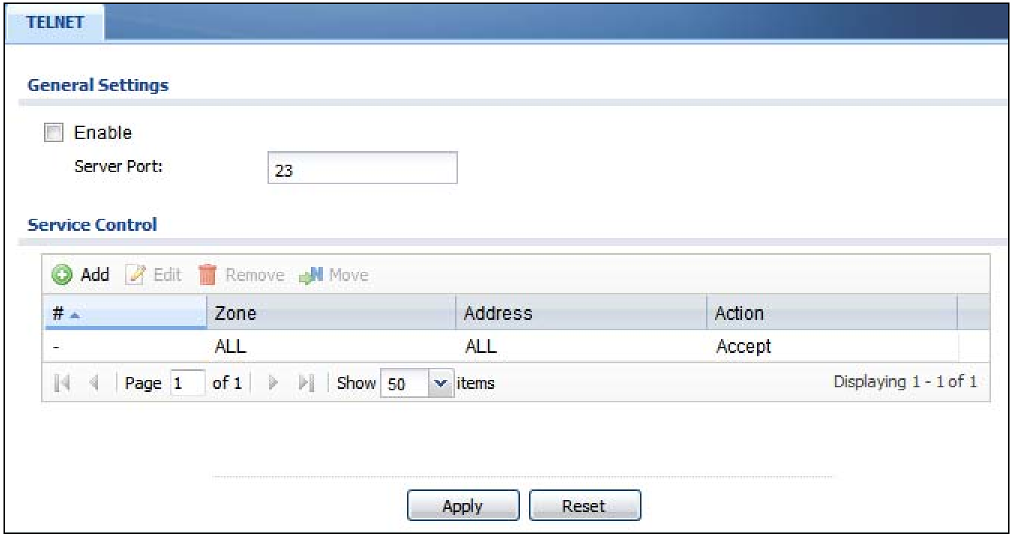
52.9 Telnet

You can use Telnet to access the ISG50's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

52.9.1 Configuring Telnet

Click **Configuration > System > TELNET** to configure your ISG50 for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the ISG50. You can also specify from which IP addresses the access can come.

Figure 476 Configuration > System > TELNET



Server Port: 23

#	Zone	Address	Action
-	ALL	ALL	Accept

The following table describes the labels in this screen.

Table 278 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ISG50 CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which ISG50 zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 275 on page 683 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.

Table 278 Configuration > System > TELNET (continued)

LABEL	DESCRIPTION
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ISG50's (non-configurable) default policy. The ISG50 applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ISG50 will not have to use the default policy.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ISG50 zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

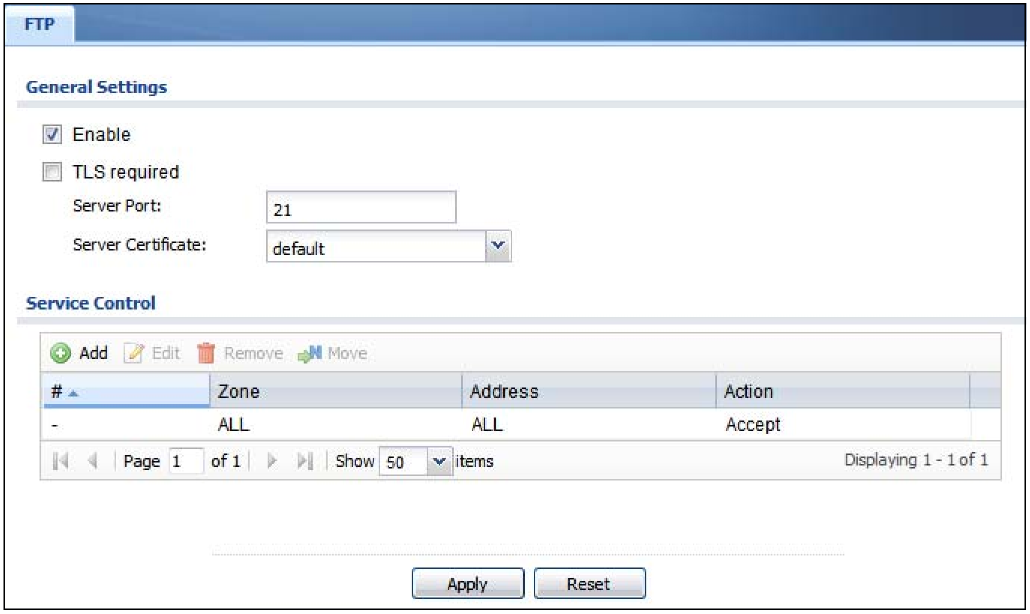
52.10 FTP

You can upload and download the ISG50's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. Please see Chapter 55 on page 725 for more information about firmware and configuration files.

52.10.1 Configuring FTP

To change your ISG50's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the ISG50. You can also specify from which IP addresses the access can come.

Figure 477 Configuration > System > FTP



☑ Enable

☐ TLS required

Server Port: 21

Server Certificate: default

#	Zone	Address	Action
-	ALL	ALL	Accept

The following table describes the labels in this screen.

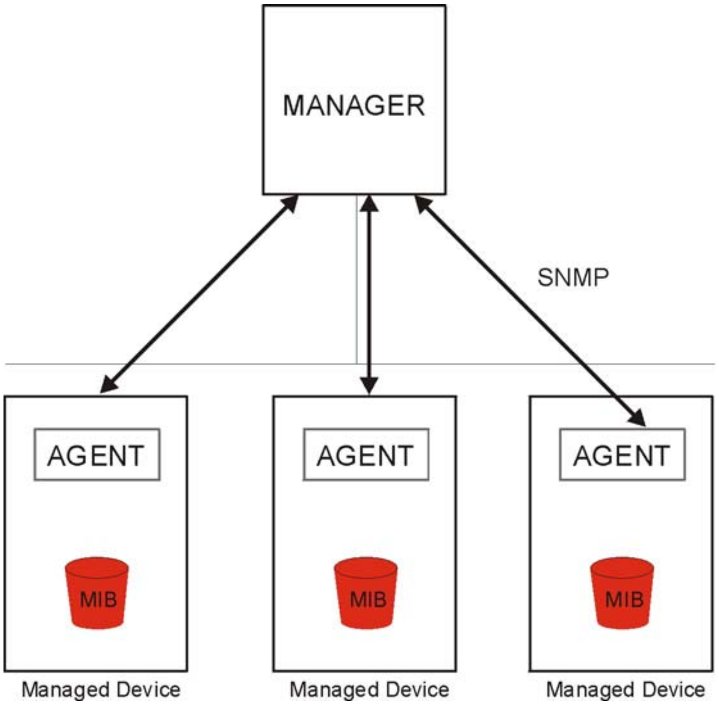
Table 279 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ISG50 using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ISG50 for FTP connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 50 on page 643 for details).
Service Control	This specifies from which computers you can access which ISG50 zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 275 on page 683 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ISG50's (non-configurable) default policy. The ISG50 applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ISG50 will not have to use the default policy.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ISG50 zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.11 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ISG50 supports SNMP agent functionality, which allows a manager station to manage and monitor the ISG50 through the network. The ISG50 supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 478 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ISG50). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

52.11.1 Supported MIBs

The ISG50 supports MIB II that is defined in RFC-1213 and RFC-1215. The ISG50 also supports private MIBs (ZYXEL-ES-SMI.mib and ZYXEL-ES_COMMON.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the ISG50's MIBs from www.zyxel.com.

52.11.2 SNMP Traps

The ISG50 will send traps to the SNMP manager when any one of the following events occurs.

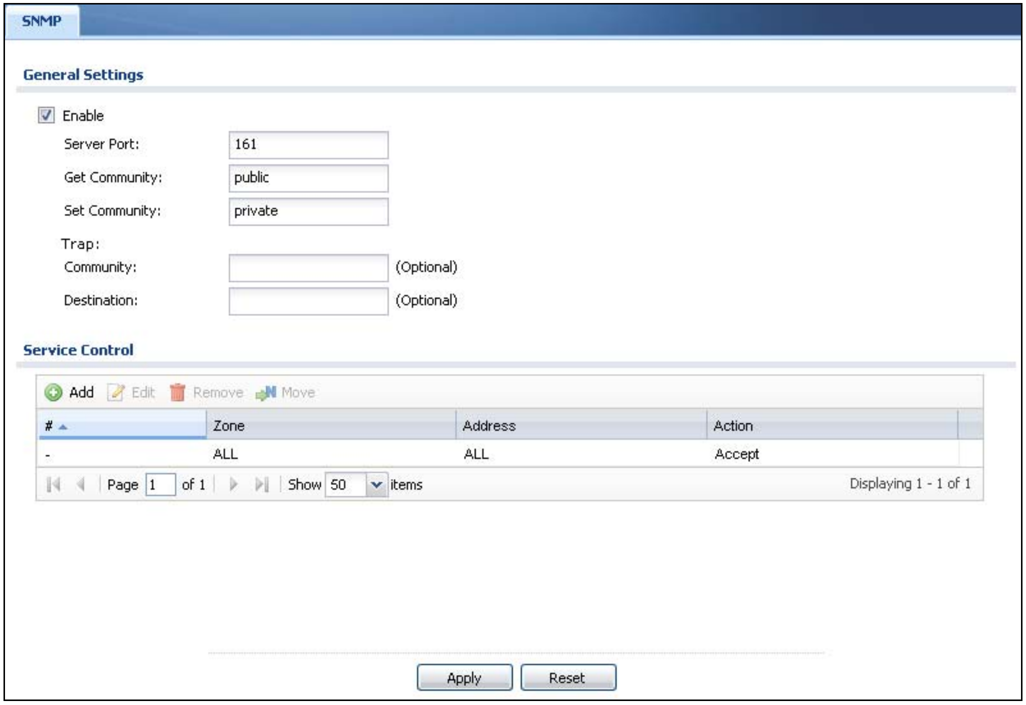
Table 280 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ISG50 is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

52.11.3 Configuring SNMP

To change your ISG50's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the ISG50. You can also specify from which IP addresses the access can come.

Figure 479 Configuration > System > SNMP



☑ Enable

Server Port: 161

Get Community: public

Set Community: private

Trap:

Community: (Optional)

Destination: (Optional)

#	Zone	Address	Action
-	ALL	ALL	Accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

The following table describes the labels in this screen.

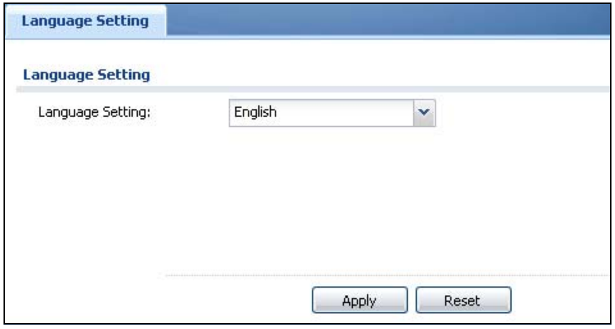
Table 281 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ISG50 using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Service Control	This specifies from which computers you can access which ISG50 zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 275 on page 683 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ISG50's (non-configurable) default policy. The ISG50 applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ISG50 will not have to use the default policy.
Zone	This is the zone on the ISG50 the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ISG50 zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

52.12 Language Screen

Click **Configuration > System > Language** to open the following screen. Use this screen to select a display language for the ISG50's Web Configurator screens.

Figure 480 Configuration > System > Language



Language Setting
Language Setting
Language Setting:
English
Apply
Reset

The following table describes the labels in this screen.

Table 282 Configuration > System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the ISG50's Web Configurator screens. You also need to open a new browser session to display the screens in the new language.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

53

Log and Report

53.1 Overview

Use these screens to configure daily reporting and log settings.

53.1.1 What You Can Do In this Chapter

- Use the **Email Daily Report** screen (Section 53.2 on page 705) to configure where and how to send daily reports and what reports to send.
- Use the **Maintenance** > **Log Setting** screens (Section 53.3 on page 707) to specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

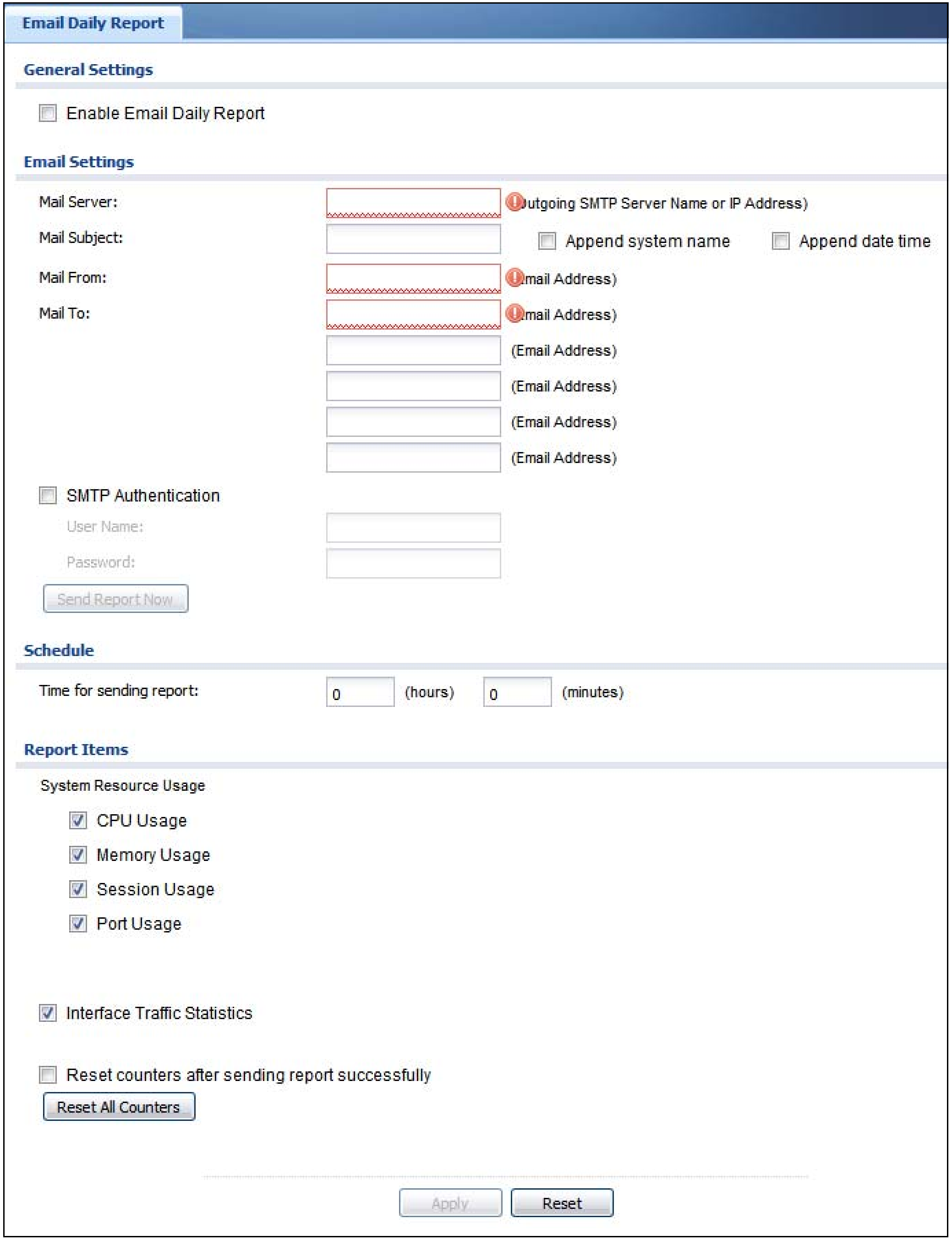
53.2 Email Daily Report

Use the **Email Daily Report** screen to start or stop data collection and view various statistics about traffic passing through your ISG50.

Note: Data collection may decrease the ISG50’s traffic throughput rate.

Click **Configuration > Log & Report > Email Daily Report** to display the following screen. Configure this screen to have the ISG50 e-mail you system statistics every day.

Figure 481 Configuration > Log & Report > Email Daily Report



Email Daily Report

General Settings

☐ Enable Email Daily Report

Email Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)
Mail Subject: ☐ Append system name ☐ Append date time
Mail From: (Email Address)
Mail To: (Email Address)
(Email Address)
(Email Address)
(Email Address)
(Email Address)

☐ SMTP Authentication
User Name:
Password:

Schedule

Time for sending report: 0 (hours) 0 (minutes)

Report Items

System Resource Usage
☑ CPU Usage
☑ Memory Usage
☑ Session Usage
☑ Port Usage

☑ Interface Traffic Statistics

☐ Reset counters after sending report successfully

The following table describes the labels in this screen.

Table 283 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by e-mail every day.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail. Select **Append system name** to add the ISG50’s system name to the subject. Select **Append date time** to add the ISG50’s system date and time to the subject.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Mail To	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Send Report Now	Click this button to have the ISG50 send the daily e-mail report immediately.
Time for sending report	Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click **Apply** to save your changes back to the ISG50.
Reset	Click **Reset** to return the screen to its last-saved settings.

53.3 Log Setting Screens

The **Log Setting** screens control log messages and alerts. A log message stores the information for viewing (for example, in the **View Log** tab) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The ISG50 provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** tab, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Setting** tab also controls what information is saved in each log. For the system log, you can also specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

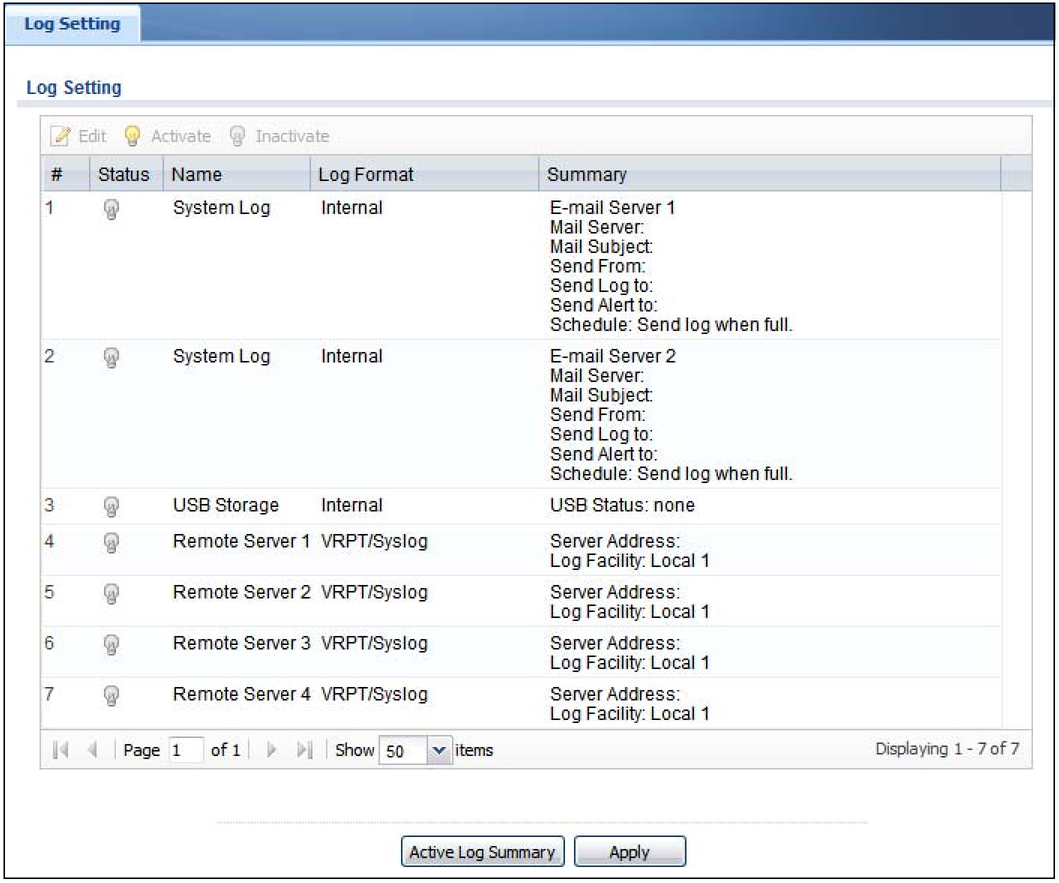
For alerts, the **Log Settings** tab controls which events generate alerts and where alerts are e-mailed.

The **Log Settings Summary** screen provides a summary of all the settings. You can use the **Log Settings Edit** screen to maintain the detailed settings (such as log categories, e-mail addresses, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

53.3.1 Log Setting Summary

To access this screen, click **Configuration > Log & Report > Log Setting**.

Figure 482 Configuration > Log & Report > Log Setting



#	Status	Name	Log Format	Summary
1		System Log	Internal	E-mail Server 1 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
2		System Log	Internal	E-mail Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3		USB Storage	Internal	USB Status: none
4		Remote Server 1	VRPT/Syslog	Server Address: Log Facility: Local 1
5		Remote Server 2	VRPT/Syslog	Server Address: Log Facility: Local 1
6		Remote Server 3	VRPT/Syslog	Server Address: Log Facility: Local 1
7		Remote Server 4	VRPT/Syslog	Server Address: Log Facility: Local 1

The following table describes the labels in this screen.

Table 284 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific log.
Name	This field displays the type of log setting entry (system log, logs stored on a connected USB storage device, or one of the remote servers).

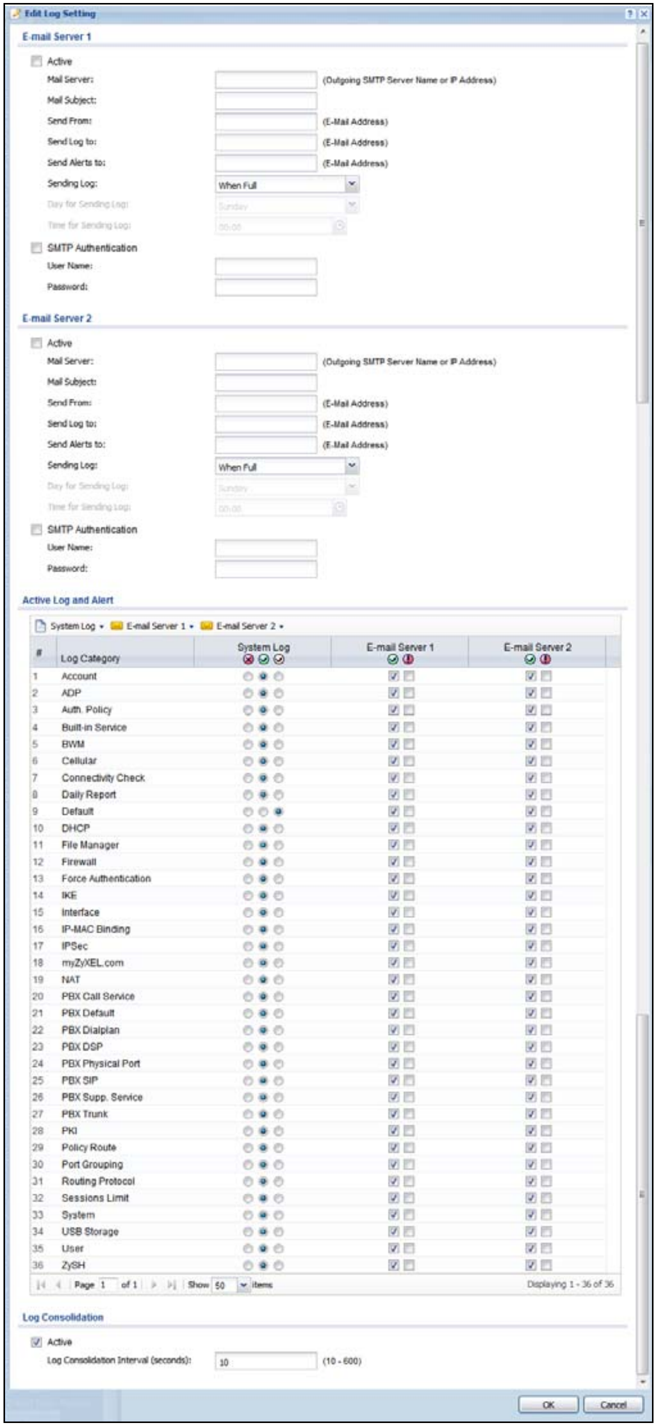
Table 284 Configuration > Log & Report > Log Setting (continued)

LABEL	DESCRIPTION
Log Format	This field displays the format of the log. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - ZyXEL's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 53.3.2 on page 710 for more information.
Active Log Summary	Click this button to open the **Active Log Summary Edit** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

53.3.2 Edit System Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the **Log Settings Summary** screen (see Section 53.3.1 on page 708), and click the system log **Edit** icon.

Figure 483 Configuration > Log & Report > Log Setting > Edit (System Log)



E-mail Server 1

☐ Active
Mail Server: (Outgoing SMTP Server Name or IP Address)
Mail Subject:
Send From: (E-Mail Address)
Send Log to: (E-Mail Address)
Send Alerts to: (E-Mail Address)
Sending Log: When Full
Day for Sending Log: Sunday
Time for Sending Log: 00:00
☐ SMTP Authentication
User Name:
Password:

E-mail Server 2

☐ Active
Mail Server: (Outgoing SMTP Server Name or IP Address)
Mail Subject:
Send From: (E-Mail Address)
Send Log to: (E-Mail Address)
Send Alerts to: (E-Mail Address)
Sending Log: When Full
Day for Sending Log: Sunday
Time for Sending Log: 00:00
☐ SMTP Authentication
User Name:
Password:

Active Log and Alert

#	Log Category	System Log	E-mail Server 1	E-mail Server 2
1	Account	○ ● ○	☑ ☐	☑ ☐
2	ADP	○ ● ○	☑ ☐	☑ ☐
3	Auth. Policy	○ ● ○	☑ ☐	☑ ☐
4	Built-in Service	○ ● ○	☑ ☐	☑ ☐
5	BWM	○ ● ○	☑ ☐	☑ ☐
6	Cellular	○ ● ○	☑ ☐	☑ ☐
7	Connectivity Check	○ ● ○	☑ ☐	☑ ☐
8	Daily Report	○ ● ○	☑ ☐	☑ ☐
9	Default	○ ○ ●	☑ ☐	☑ ☐
10	DHCP	○ ● ○	☑ ☐	☑ ☐
11	File Manager	○ ● ○	☑ ☐	☑ ☐
12	Firewall	○ ● ○	☑ ☐	☑ ☐
13	Force Authentication	○ ● ○	☑ ☐	☑ ☐
14	IKE	○ ● ○	☑ ☐	☑ ☐
15	Interface	○ ● ○	☑ ☐	☑ ☐
16	IP-MAC Binding	○ ● ○	☑ ☐	☑ ☐
17	IPSec	○ ● ○	☑ ☐	☑ ☐
18	myZyXEL.com	○ ● ○	☑ ☐	☑ ☐
19	NAT	○ ● ○	☑ ☐	☑ ☐
20	PBX Call Service	○ ● ○	☑ ☐	☑ ☐
21	PBX Default	○ ● ○	☑ ☐	☑ ☐
22	PBX Dialplan	○ ● ○	☑ ☐	☑ ☐
23	PBX DSP	○ ● ○	☑ ☐	☑ ☐
24	PBX Physical Port	○ ● ○	☑ ☐	☑ ☐
25	PBX SIP	○ ● ○	☑ ☐	☑ ☐
26	PBX Supp. Service	○ ● ○	☑ ☐	☑ ☐
27	PBX Trunk	○ ● ○	☑ ☐	☑ ☐
28	PKI	○ ● ○	☑ ☐	☑ ☐
29	Policy Route	○ ● ○	☑ ☐	☑ ☐
30	Port Grouping	○ ● ○	☑ ☐	☑ ☐
31	Routing Protocol	○ ● ○	☑ ☐	☑ ☐
32	Sessions Limit	○ ● ○	☑ ☐	☑ ☐
33	System	○ ● ○	☑ ☐	☑ ☐
34	USB Storage	○ ● ○	☑ ☐	☑ ☐
35	User	○ ● ○	☑ ☐	☑ ☐
36	ZySH	○ ● ○	☑ ☐	☑ ☐

Page 1 of 1 | Show 50 items | Displaying 1 - 36 of 36

Log Consolidation

☑ Active
Log Consolidation Interval (seconds): 10 (10 - 600)

The following table describes the labels in this screen.

Table 285 Configuration > Log & Report > Log Setting > Edit (System Log)

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**.
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Active Log and Alert	
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the ISG50 will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The ISG50 does not e-mail debugging information, even if this setting is selected.
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.

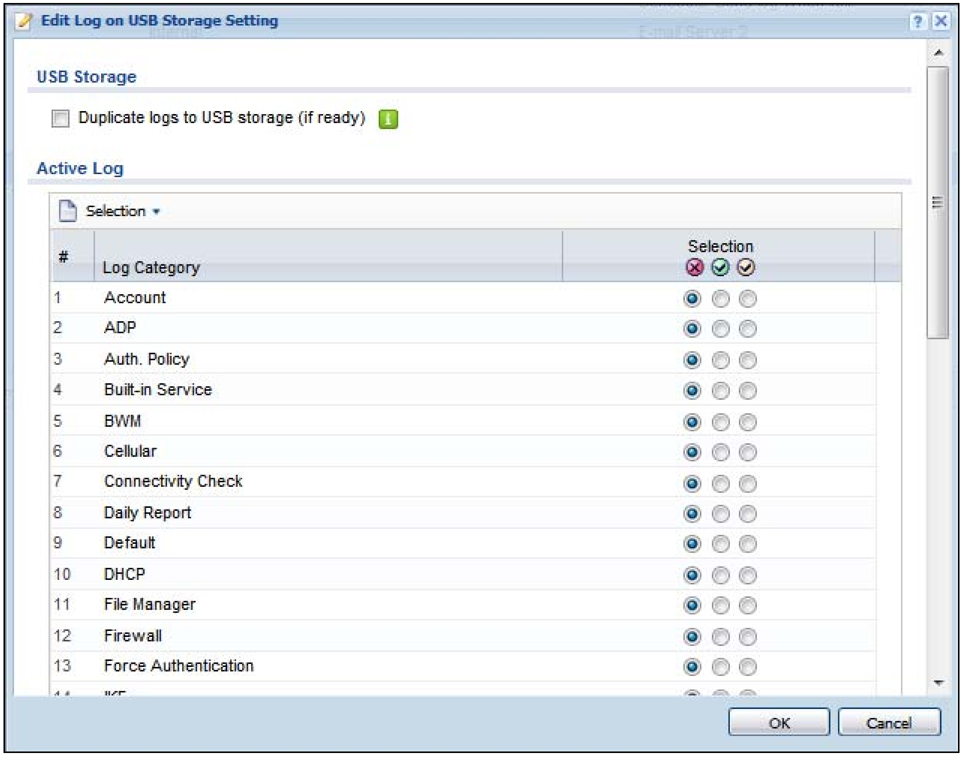
Table 285 Configuration > Log & Report > Log Setting > Edit (System Log) (continued)

LABEL	DESCRIPTION
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the ISG50 does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The ISG50 does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The ISG50 does not e-mail debugging information, even if it is recorded in the **System log**.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

53.3.3 Edit Log on USB Storage Setting

The **Edit Log on USB Storage Setting** screen controls the detailed settings for saving logs to a connected USB storage device. Go to the **Log Setting Summary** screen (see Section 53.3.1 on page 708, and click the **USB storage Edit** icon.

Figure 484 Configuration > Log & Report > Log Setting > Edit (USB Storage)



USB Storage

☐ Duplicate logs to USB storage (if ready)

Active Log

Selection ▾

#	Log Category	Selection ⊗	✓	✓
1	Account	●	○	○
2	ADP	●	○	○
3	Auth. Policy	●	○	○
4	Built-in Service	●	○	○
5	BWM	●	○	○
6	Cellular	●	○	○
7	Connectivity Check	●	○	○
8	Daily Report	●	○	○
9	Default	●	○	○
10	DHCP	●	○	○
11	File Manager	●	○	○
12	Firewall	●	○	○
13	Force Authentication	●	○	○

The following table describes the labels in this screen.

Table 286 Configuration > Log & Report > Log Setting > Edit (USB Storage)

LABEL	DESCRIPTION
Duplicate logs to USB storage (if ready)	Select this to have the ISG50 save a copy of its system logs to a connected USB storage device. Use the **Active Log** section to specify what kinds of messages to include.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. The **Default** category includes debugging messages generated by open source software.

Table 286 Configuration > Log & Report > Log Setting > Edit (USB Storage) (continued)

LABEL	DESCRIPTION
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

53.3.4 Edit Remote Server Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see Section 53.3.1 on page 708), and click a remote server **Edit** icon.

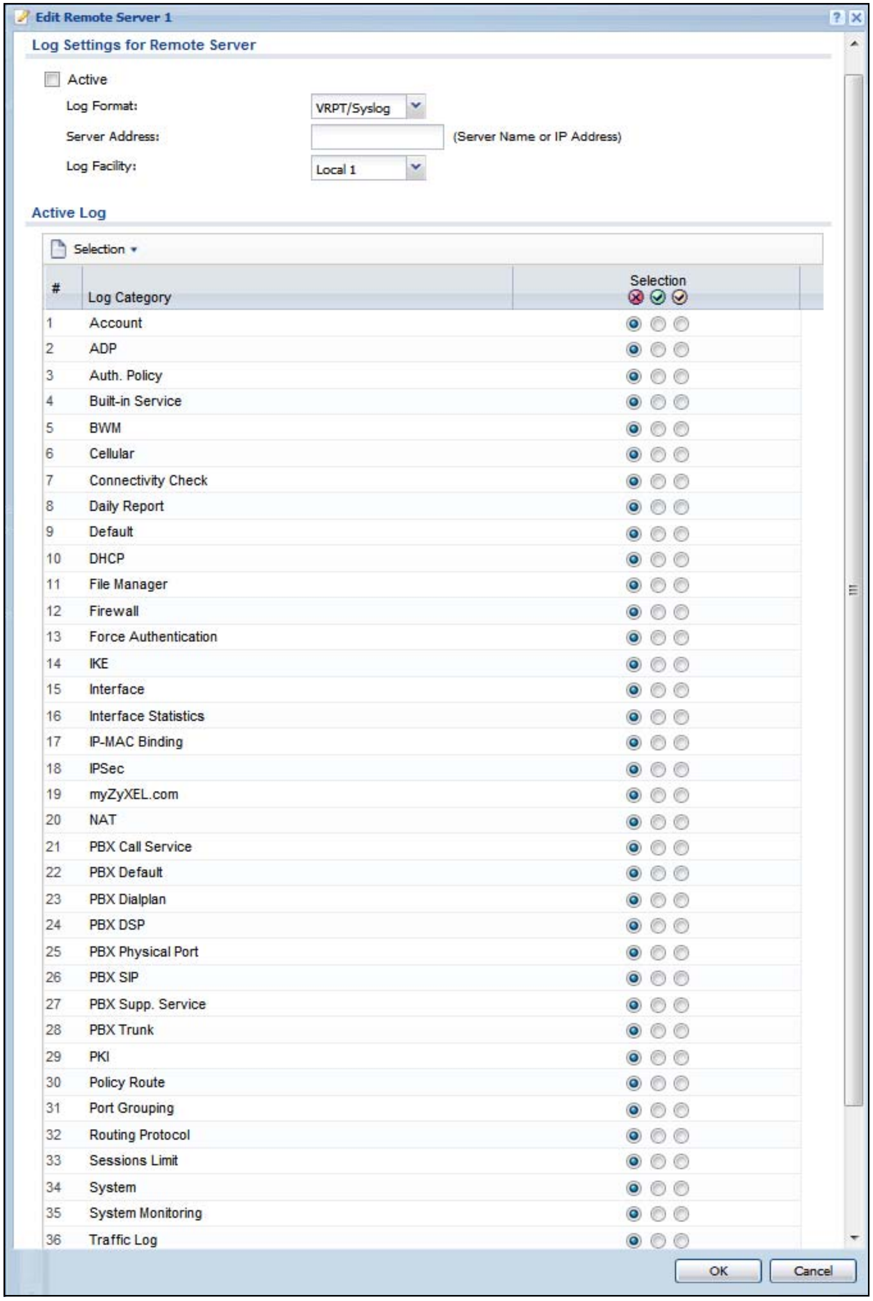


Figure 485 Configuration > Log & Report > Log Setting > Edit (Remote Server)

☐ Active

Log Format: VRPT/Syslog

Server Address: (Server Name or IP Address)

Log Facility: Local 1

#	Log Category	Selection
1	Account	● ○ ○
2	ADP	● ○ ○
3	Auth. Policy	● ○ ○
4	Built-in Service	● ○ ○
5	BWM	● ○ ○
6	Cellular	● ○ ○
7	Connectivity Check	● ○ ○
8	Daily Report	● ○ ○
9	Default	● ○ ○
10	DHCP	● ○ ○
11	File Manager	● ○ ○
12	Firewall	● ○ ○
13	Force Authentication	● ○ ○
14	IKE	● ○ ○
15	Interface	● ○ ○
16	Interface Statistics	● ○ ○
17	IP-MAC Binding	● ○ ○
18	IPSec	● ○ ○
19	myZyXEL.com	● ○ ○
20	NAT	● ○ ○
21	PBX Call Service	● ○ ○
22	PBX Default	● ○ ○
23	PBX Dialplan	● ○ ○
24	PBX DSP	● ○ ○
25	PBX Physical Port	● ○ ○
26	PBX SIP	● ○ ○
27	PBX Supp. Service	● ○ ○
28	PBX Trunk	● ○ ○
29	PKI	● ○ ○
30	Policy Route	● ○ ○
31	Port Grouping	● ○ ○
32	Routing Protocol	● ○ ○
33	Sessions Limit	● ○ ○
34	System	● ○ ○
35	System Monitoring	● ○ ○
36	Traffic Log	● ○ ○

The following table describes the labels in this screen.

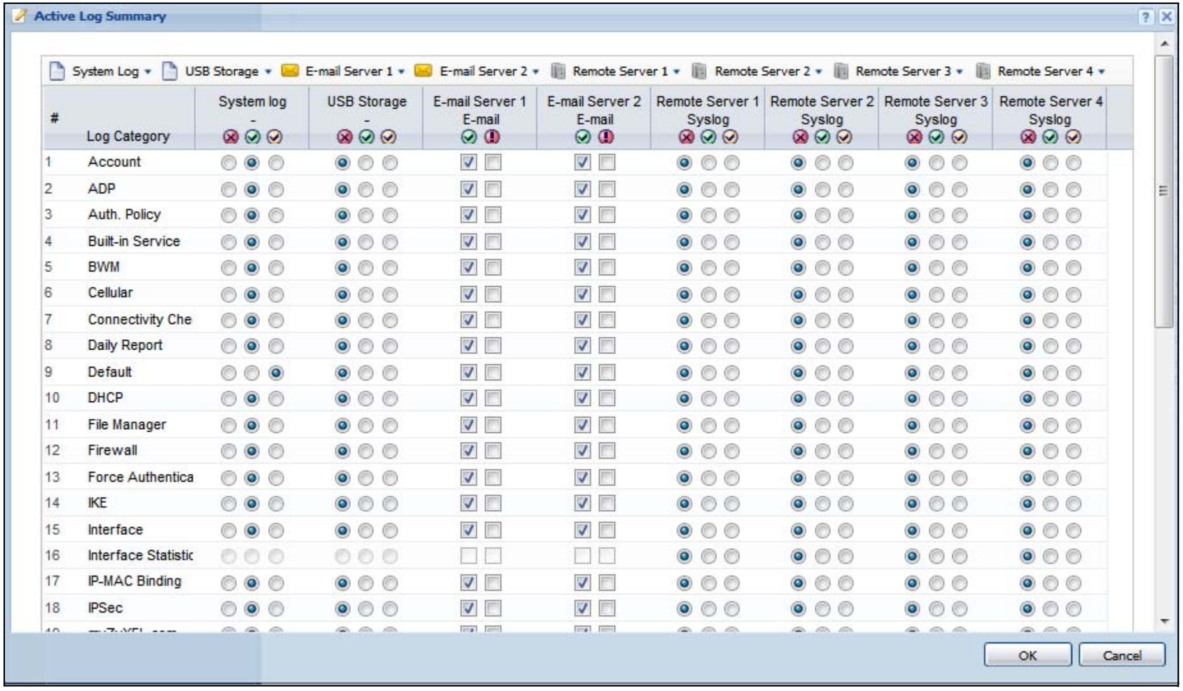
Table 287 Configuration > Log & Report > Log Setting > Edit (Remote Server)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT / Syslog** - ZyXEL's Vantage Report, syslog-compatible format. **CEF / Syslog** - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

53.3.5 Active Log Summary Screen

The **Active Log Summary** screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names).To access this screen, go to the **Log Settings Summary** screen (see Section 53.3.1 on page 708), and click the **Active Log Summary** button.

Figure 486 Active Log Summary



#	Log Category	System log - ⊗ ✓ ✓	USB Storage - ⊗ ✓ ✓	E-mail Server 1 E-mail ✓ !	E-mail Server 2 E-mail ✓ !	Remote Server 1 Syslog ⊗ ✓ ✓	Remote Server 2 Syslog ⊗ ✓ ✓	Remote Server 3 Syslog ⊗ ✓ ✓	Remote Server 4 Syslog ⊗ ✓ ✓
1	Account	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
2	ADP	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
3	Auth. Policy	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
4	Built-in Service	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
5	BWM	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
6	Cellular	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
7	Connectivity Che	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
8	Daily Report	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
9	Default	○ ○ ●	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
10	DHCP	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
11	File Manager	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
12	Firewall	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
13	Force Authentica	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
14	IKE	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
15	Interface	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
16	Interface Statistic	○ ○ ○	○ ○ ○	☐ ☐	☐ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
17	IP-MAC Binding	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○
18	IPSec	○ ● ○	● ○ ○	☑ ☐	☑ ☐	● ○ ○	● ○ ○	● ○ ○	● ○ ○

This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 53.3.2 on page 710, where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 288 Configuration > Log & Report > Log Setting > Active Log Summary

LABEL	DESCRIPTION
System Log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the ISG50 will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The ISG50 does not e-mail debugging information, even if this setting is selected.
USB Storage	Use the **USB Storage** drop-down list to change the log settings for saving logs to a connected USB storage device. **disable all logs** (red X) - do not log any information for any category to a connected USB storage device. **enable normal logs** (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories and save them to a connected USB storage device.

Table 288 Configuration > Log & Report > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the ISG50 does not e-mail debugging information, however, even if this setting is selected.
USB Storage	Select whether each category of events should be included in the log messages saved to a connected USB storage device.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The ISG50 does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The ISG50 does not e-mail debugging information, even if it is recorded in the **System log**.

Table 288 Configuration > Log & Report > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
Remote Server 1~4	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

Call Detail Record (CDR)

54.1 Overview

This chapter shows you how to collect and manage Call Detail Records (CDRs) on the ISG50.

Call Detail Records (CDRs) are telephone records containing details such as the time of call, duration of call, source telephone number and so on. The ISG50 has a built in CDR database that automatically stores calls made to or from its extensions. You can search the CDR database to find out details about your organization's calls. You can also use an external database to store CDRs.

54.1.1 What You Can Do in this Chapter

- Use the **CDR Configuration** screen to configure where to store CDR information, an administrator e-mail address to send alerts and CDR backup files for later viewing. See Section 54.2 on page 721.

54.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Local CDR Database

The local CDR database has limited capacity and when it is full it empties its contents into a compressed file of the call records. This file is referred to as an "Aged File". You can delete an "Aged File" or forward it to an e-mail address where it can be reviewed at a later time. The CDR database is then emptied. Whether you delete the aged file or send to an administrator, the ISG50 continues to record telephone call details in an empty CDR database.

Another way to deal with the limited capacity on the local CDR database of the ISG50 is to actively manage the CDR database. This requires you to create backups of the CDR database and send them to an administrator via e-mail.

Viewing Aged Files

An "Aged File" is a compressed file with the extension ".tgz". ".tgz" files can be decompressed with data compression utilities for example 7-Zip. The result of decompressing this file are cdr.xxxxx.sql or cdr.xxxxx.csv files. The .sql files can be managed via a PostgreSQL Database Management System (DBMS).

CDR Database Management via PostgreSQL

PostgreSQL is a database management system based on SQL (Structured Query Language). You can configure a PostgreSQL server to collect CDRs from the ISG50 and expand the capacity of telephone records you can collect and review.

54.2 The CDR Configuration Screen

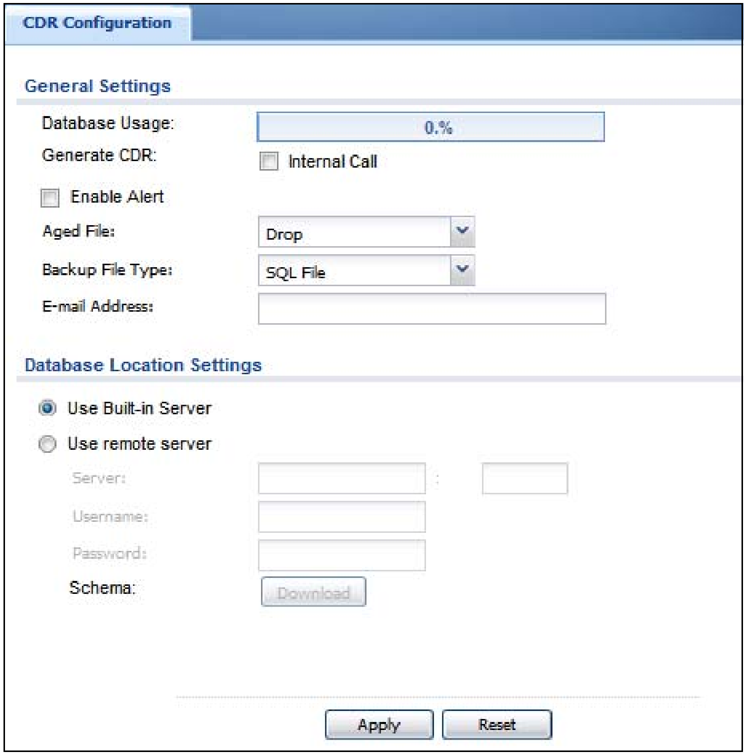
Use this screen to set up an external server to collect CDR information. You can also configure an administration e-mail address to which to send alerts and CDR files for later viewing.

Note: You should use a PostgreSQL server 8.0 or above for the remote server.

You must execute the SQL script downloaded from this screen on your PostgreSQL server before the ISG50 starts to work with the remote server.

Click **Report > LOGS > CDR > Configuration** to view the screen as shown next.

Figure 487 Report > LOGS > CDR > Configuration



Database Usage: 0.%

Generate CDR: ☐ Internal Call

☐ Enable Alert

Aged File: Drop

Backup File Type: SQL File

E-mail Address:

● Use Built-in Server

○ Use remote server

Server: :

Username:

Password:

Schema:

Each field is described in the following table.

Table 289 CDR > Configuration

LABEL	DESCRIPTION
CDR Setting	
Database Usage	This field indicates the percentage of records currently held by the database. When the local database is full, the ISG50 removes all the CDRs from the local database and creates an "Aged File" (a compressed file containing all the CDRs). Use the **Aged File** field to specify how to deal with the compressed file containing the CDRs.
Generate CDR	Select this to record internal calls. Internal calls are calls from one extension to another extension configured on the ISG50. Clear this box if you do not want the ISG50 to record internal calls.
Enable Alert	Select this to have the ISG50 send an email alert to the e-mail address specified in the **E-mail Address** field when the CDR database is half full.
Aged File	Specify how to deal with CDR files when the CDR database is full. Choose **mail to admin.** to send the CDR file to the e-mail address specified in the **E-mail Address** field and then delete it or **drop** to delete the file from the system.
Backup File Type	Select whether you want the ISG50 to send a SQL database file or a CSV file.
E-mail Address	Type the e-mail address to which you want to send the alerts indicating that the CDR file is half full. This is also the e-mail address to which complete CDR files are sent when they are full (reach approximately 10000 records).
Database Location	Use this section to specify the location and login credentials for a PostgreSQL server that collects the CDR information from the ISG50.
Use Built-in Server	Select this to have the ISG50 uses the built-in PostgreSQL server to collect CDR information.
Use remote server	Select this to have the ISG50 send a record of each call to the remote PostgreSQL server you specify in the **Server** field.
Server	Type the IP address or the domain name of the server to which you want to send your CDR files. Then type the port number on which the remote server receives records of telephone calls from the ISG50.
Username	Type the username of the account set up on a remote server to which you want to send your CDR files.
Password	Type the password of the account set up on a remote server to which you want to send your CDR files.
Schema	Click **Download** to download a SQL script (cdr.sql). Execute the script in your external database server to establish a database to work with your ISG50.
Apply	Click the **Apply** button to save your changes.

54.2.1 Configure Your Remote Server

The procedure to configure your remote server is as follows:

1 In the **Report > LOGS > CDR > Configuration** screen select **Use remote server** and click **Download**.

2 Save the **cdr.sql** file to your computer.

3 Add the following entry in "PostgreSQL installed directory"/data/pg_hba.conf file:

host all all ISG50_IP_Address/32 trust

4 Restart the PostgreSQL database server.

5 Move the cdr.sql file to “PostgreSQL installed directory”/bin and change to this directory and execute the following command:

```
psql -h localhost -U sqlzyxel < cdr.sql
```

6 After the script is successfully applied, your PostgreSQL server can work with the ISG50.

55

File Manager

55.1 Overview

Configuration files define the ISG50's settings. Shell scripts are files of commands that you can store on the ISG50 and run when you need them. You can apply a configuration file or run a shell script without the ISG50 restarting. You can store multiple configuration files and shell script files on the ISG50. You can edit configuration files or shell scripts in a text editor and upload them to the ISG50. Configuration files use a .conf extension and shell scripts use a .zysh extension.

55.1.1 What You Can Do in this Chapter

- Use the **Configuration File** screen (see Section 55.2 on page 727) to store and name configuration files. You can also download configuration files from the ISG50 to your computer and upload configuration files from your computer to the ISG50.
- Use the **Firmware Package** screen (see Section 55.3 on page 731) to check your current firmware version and upload firmware to the ISG50.
- Use the **Shell Script** screen (see Section 55.4 on page 733) to store, name, download, upload and run shell script files.

55.1.2 What you Need to Know

Configuration Files and Shell Scripts

When you apply a configuration file, the ISG50 uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the ISG50 only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 488 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure lan1
interface lan1
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-Device firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-Device firewall for TW_TEAM for remote management
firewall WAN Device insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ISG50 applies configuration files differently than it runs shell scripts. This is explained below.

Table 290 Configuration Files and Shell Scripts in the ISG50

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the example in Figure 488 on page 726 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ISG50 treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ISG50 exit sub command mode.

Note: “exit” or “!'” must follow sub commands if it is to make the ISG50 exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface wan1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface wan1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2008/04/05
interface wan1
ip address dhcp
!
```

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ISG50 processes the file line-by-line. The ISG50 checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ISG50 finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ISG50 ignores any errors in the configuration file or shell script and applies all of the valid commands. The ISG50 still generates a log for any errors.

55.2 The Configuration File Screen

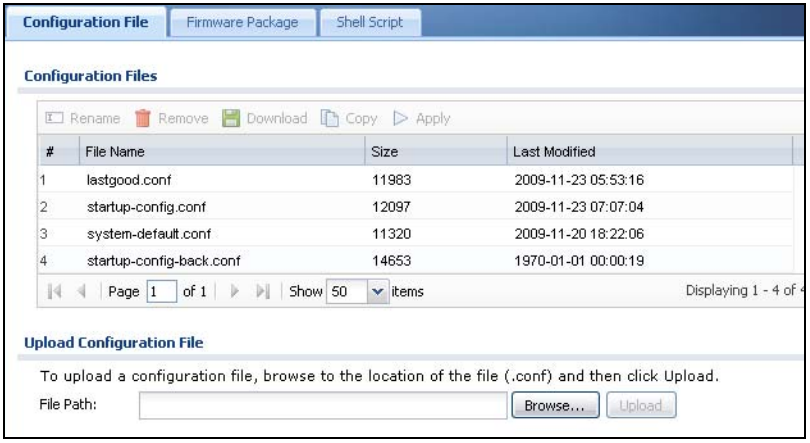
Click **Maintenance > File Manager > Configuration File** to open the **Configuration File** screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the ISG50 to your computer and upload configuration files from your computer to the ISG50.

Once your ISG50 is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the ISG50 (whether through a management interface or by physically turning the power off and back on), the ISG50 uses the **system-default.conf** configuration file with the ISG50's default settings.
- If there is a **startup-config.conf**, the ISG50 checks it for errors and applies it. If there are no errors, the ISG50 uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the ISG50 generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ISG50 applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ISG50 ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ISG50 still generates a log for any errors.

Figure 489 Maintenance > File Manager > Configuration File


Configuration File
Firmware Package
Shell Script
Configuration Files
Rename
Remove
Download
Copy
Apply

#	File Name	Size	Last Modified
1	lastgood.conf	11983	2009-11-23 05:53:16
2	startup-config.conf	12097	2009-11-23 07:07:04
3	system-default.conf	11320	2009-11-20 18:22:06
4	startup-config-back.conf	14653	1970-01-01 00:00:19

Page 1 of 1
Show 50 items
Displaying 1 - 4 of
Upload Configuration File

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path:
Browse...
Upload

Do not turn off the ISG50 while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 291 Maintenance > File Manager > Configuration File

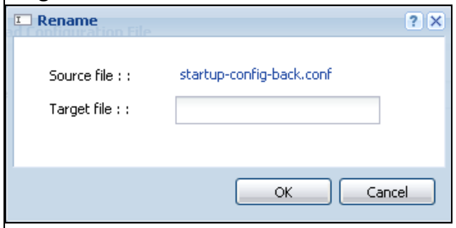
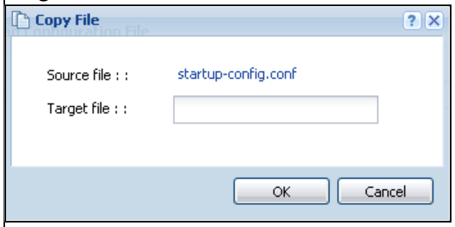
LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the ISG50. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the ISG50. Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen. **Figure 490** Maintenance > File Manager > Configuration File > Rename  Source file : : startup-config-back.conf Target file : : Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the ISG50. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the ISG50. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen. **Figure 491** Maintenance > File Manager > Configuration File > Copy  Source file : : startup-config.conf Target file : : Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 291 Maintenance > File Manager > Configuration File (continued)

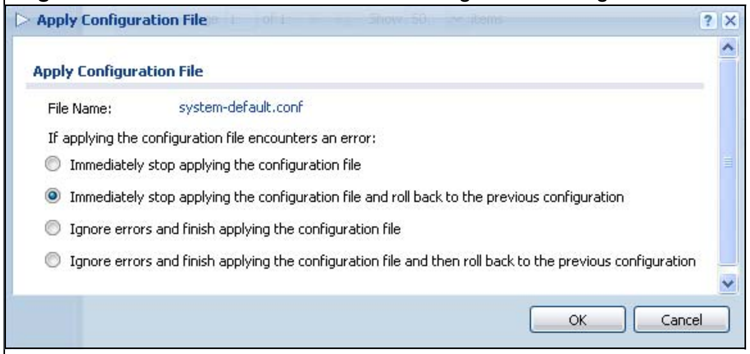
LABEL	DESCRIPTION
Apply	Use this button to have the ISG50 use a specific configuration file. Click a configuration file's row to select it and click **Apply** to have the ISG50 use that configuration file. The ISG50 does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the ISG50 is to do if it encounters an error in the configuration file. **Figure 492** Maintenance > File Manager > Configuration File > Apply  Apply Configuration File Apply Configuration File File Name: system-default.conf If applying the configuration file encounters an error: ○ Immediately stop applying the configuration file ● Immediately stop applying the configuration file and roll back to the previous configuration ○ Ignore errors and finish applying the configuration file ○ Ignore errors and finish applying the configuration file and then roll back to the previous configuration **Immediately stop applying the configuration file** - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the ISG50 started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the ISG50 apply most of your configuration and you can refer to the logs for what to fix. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the ISG50 with a fully valid configuration file. Click **OK** to have the ISG50 start applying the configuration file or click **Cancel** to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.

Table 291 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the ISG50's default settings. Select this file and click **Apply** to reset all of the ISG50 settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the ISG50 is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The ISG50 applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your ISG50 You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

55.3 The Firmware Package Screen

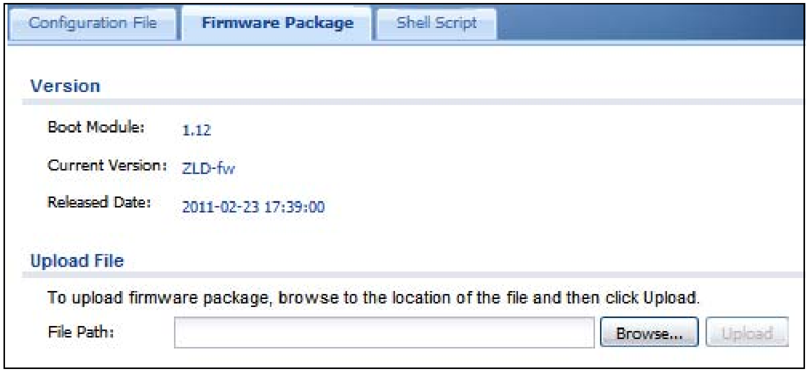
Click **Maintenance > File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the ISG50.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "ISG50.bin".

The firmware update can take up to five minutes. Do not turn off or reset the ISG50 while the firmware update is in progress!

Figure 493 Maintenance > File Manager > Firmware Package



Version

Boot Module: 1.12

Current Version: ZLD-fw

Released Date: 2011-02-23 17:39:00

Upload File

To upload firmware package, browse to the location of the file and then click Upload.

File Path:

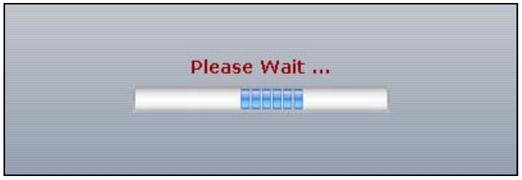
The following table describes the labels in this screen.

Table 292 Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the ISG50.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ISG50 again.

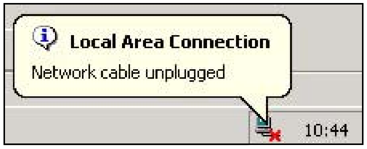
Figure 494 Firmware Upload In Process



Note: The ISG50 automatically reboots after a successful upload.

The ISG50 automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 495 Network Temporarily Disconnected



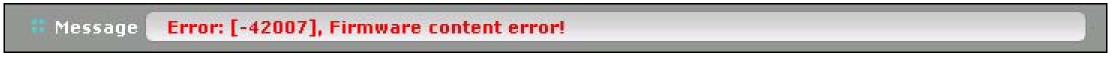
Local Area Connection

Network cable unplugged

After five minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

Figure 496 Firmware Upload Error



Error: [-42007], Firmware content error!

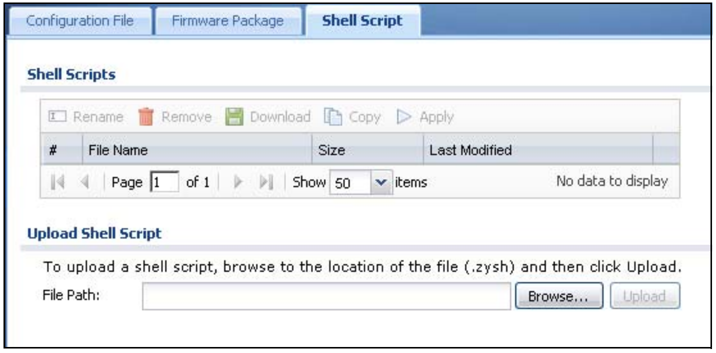
55.4 The Shell Script Screen

Use shell script files to have the ISG50 use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open the **Shell Script** screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the ISG50 at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the ISG50 restarts. You could use multiple `write` commands in a long script.

Figure 497 Maintenance > File Manager > Shell Script


Configuration File
Firmware Package
Shell Script
Shell Scripts
Rename
Remove
Download
Copy
Apply
#
File Name
Size
Last Modified
Page 1 of 1
Show 50 items
Upload Shell Script
File Path:
Browse...
Upload

No data to display

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

Each field is described in the following table.

Table 293 Maintenance > File Manager > Shell Script

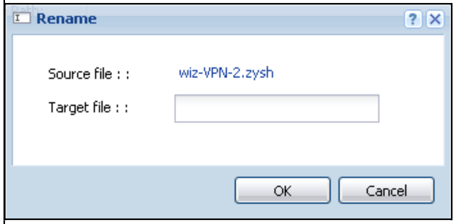
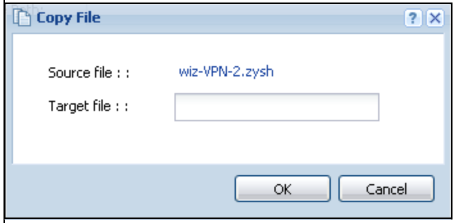
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the ISG50. You cannot rename a shell script to the name of another shell script in the ISG50. Click a shell script’s row to select it and click **Rename** to open the **Rename File** screen. **Figure 498** Maintenance > File Manager > Shell Script > Rename  Source file : : wiz-VPN-2.zysh Target file : : Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file’s row to select it and click **Remove** to delete the shell script file from the ISG50. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file’s row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the ISG50. Click a shell script file’s row to select it and click **Copy** to open the **Copy File** screen. **Figure 499** Maintenance > File Manager > Shell Script > Copy  Source file : : wiz-VPN-2.zysh Target file : : Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;‘~!@#$%^&()_+[]{}’,.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the ISG50 use a specific shell script file. Click a shell script file’s row to select it and click **Apply** to have the ISG50 use that shell script file. You may need to wait awhile for the ISG50 to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.

Table 293 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your ISG50.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

56

Diagnostics

56.1 Overview

Use the diagnostics screens for troubleshooting.

56.1.1 What You Can Do in this Chapter

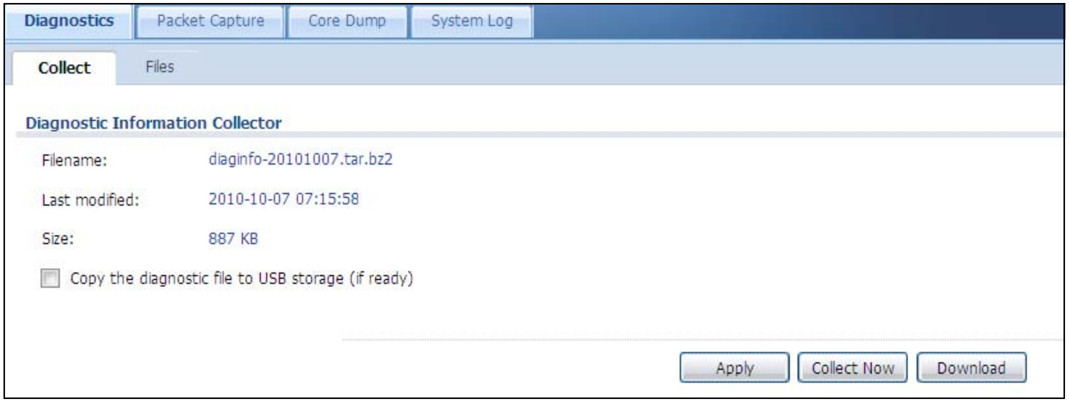
- Use the **Maintenance > Diagnostics** screen (see Section 56.2 on page 737) to generate a file containing the ISG50's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the **Maintenance > Diagnostics > Packet Capture** screens (see Section 56.3 on page 739) to capture packets going through the ISG50.
- Use the **Maintenance > Diagnostics > Core Dump** screens (see Section 56.4 on page 742) to have the ISG50 save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes) so you can send the file to customer support for troubleshooting.
- Use the **Maintenance > Diagnostics > System Log** screens (see Section 56.5 on page 744) to download files of system logs from a connected USB storage device to your computer.

56.2 The Diagnostic Screen

The **Diagnostic** screen provides an easy way for you to generate a file containing the ISG50's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

Click **Maintenance > Diagnostics** to open the **Diagnostic** screen.

Figure 500 Maintenance > Diagnostics



Filename: diaginfo-20101007.tar.bz2

Last modified: 2010-10-07 07:15:58

Size: 887 KB

☐ Copy the diagnostic file to USB storage (if ready)

The following table describes the labels in this screen.

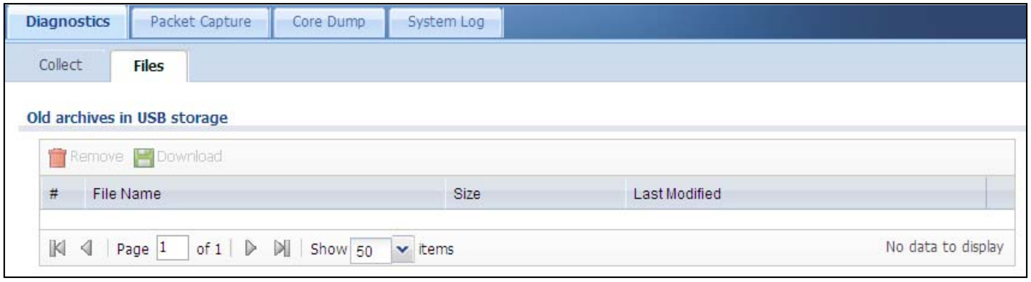
Table 294 Maintenance > Diagnostics

LABEL	DESCRIPTION
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Copy the diagnostic file to USB storage (if ready)	Select this to have the ISG50 create an extra copy of the diagnostic file to a connected USB storage device.
Apply	Click **Apply** to save your changes.
Collect Now	Click this to have the ISG50 create a new diagnostic file.
Download	Click this to save the most recent diagnostic file to a computer.

56.2.1 The Diagnostics Files Screen

Click **Maintenance > Diagnostics > Files** to open the diagnostic files screen. This screen lists the files of diagnostic information the ISG50 has collected and stored in a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 501 Maintenance > Diagnostics > Files



No data to display

The following table describes the labels in this screen.

Table 295 Maintenance > Diagnostics > Files

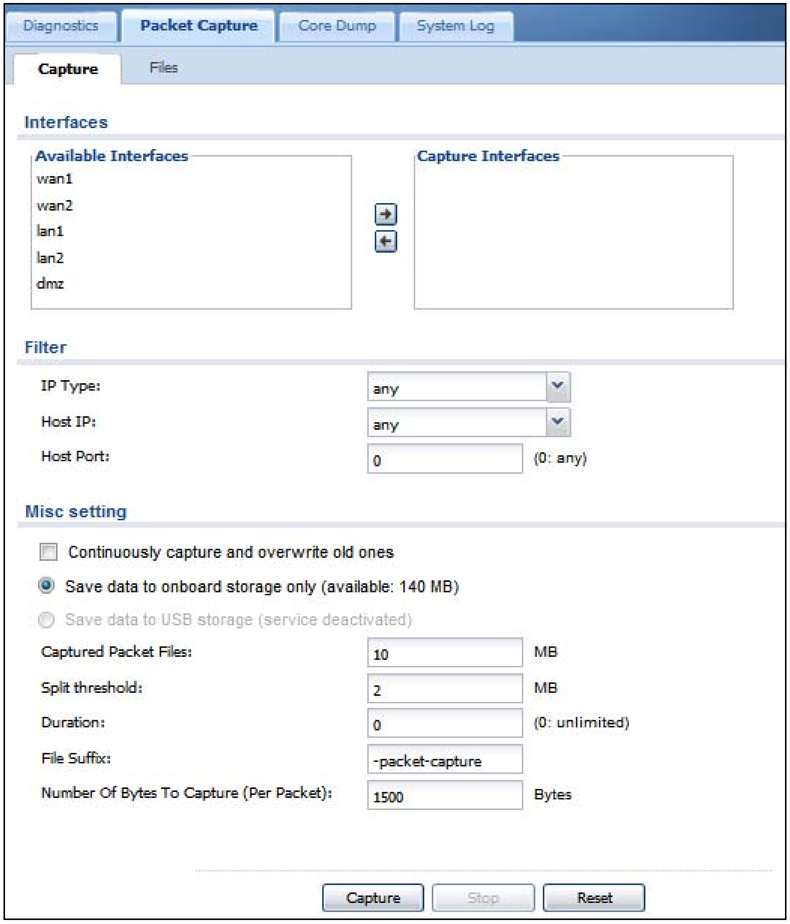
LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ISG50. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

56.3 The Packet Capture Screen

Use this screen to capture network traffic going through the ISG50’s interfaces. Studying these packet captures may help you identify network problems. Click **Maintenance > Diagnostics > Packet Capture** to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the **File Suffix** field’s setting to avoid this.

Figure 502 Maintenance > Diagnostics > Packet Capture



Available Interfaces: wan1, wan2, lan1, lan2, dmz

IP Type: any

Host IP: any

Host Port: 0 (0: any)

☐ Continuously capture and overwrite old ones

● Save data to onboard storage only (available: 140 MB)

○ Save data to USB storage (service deactivated)

Captured Packet Files: 10 MB

Split threshold: 2 MB

Duration: 0 (0: unlimited)

File Suffix: -packet-capture

Number Of Bytes To Capture (Per Packet): 1500 Bytes

The following table describes the labels in this screen.

Table 296 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Interfaces	Enabled interfaces (except for virtual interfaces) appear under **Available Interfaces**. Select interfaces for which to capture packets and click the right arrow button to move them to the **Capture Interfaces** list. Use the [Shift] and/or [Ctrl] key to select multiple objects.
IP Type	Select the protocol of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.
Host IP	Select a host IP address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.

Table 296 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Host Port	This field is configurable when you set the **IP Type** to **any**, **tcp**, or **udp**. Specify the port number of traffic to capture.
Continuously capture and overwrite old ones	Select this to have the ISG50 keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.
Save data to onboard storage only	Select this to have the ISG50 only store packet capture entries on the ISG50.
Save data to USB storage	Select this to have the ISG50 store packet capture entries only on a USB storage device connected to the ISG50. Status: **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the ISG50 cannot mount it. **none** - no USB storage device is connected. **available** - you can have the ISG50 use the USB storage device. The available storage capacity also displays. Note: The ISG50 reserves some USB storage space as a buffer.
Captured Packet Files	When saving packet captures only to the ISG50's onboard storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the ISG50. When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file. Note: If you have existing capture files and have not selected the **Continuously capture and overwrite old ones** option, you may need to set this size larger or delete existing capture files. The valid range is 1 to 10000. The ISG50 stops the capture and generates the capture file when either the file reaches this size or the time period specified in the **Duration** field expires.
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the ISG50 starts another packet capture file.
Duration	Set a time limit in seconds for the capture. The ISG50 stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified in the **File Size** field. 0 means there is no time limit.
File Suffix	Specify text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
Number Of Bytes To Capture (Per Packet)	Specify the maximum number of bytes to capture per packet. The ISG50 automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.

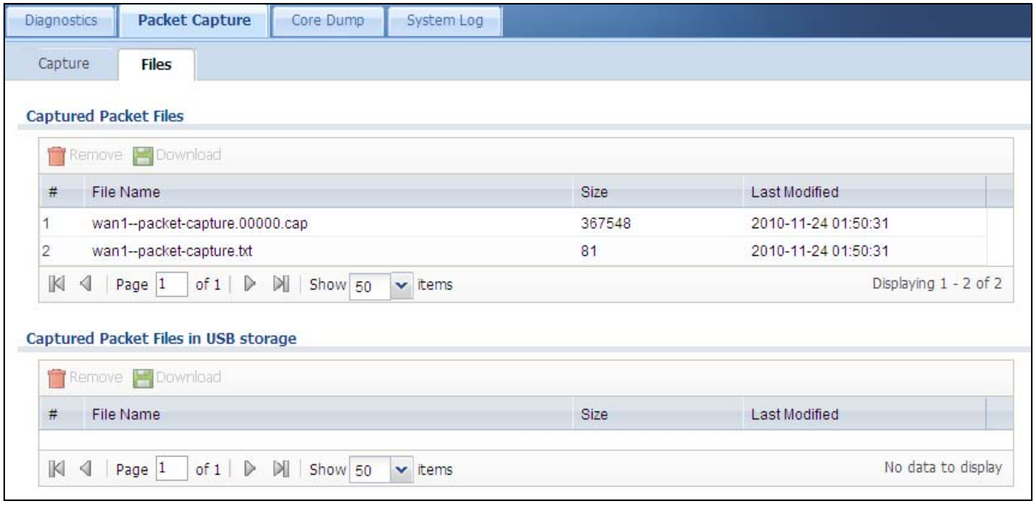
Table 296 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Capture	Click this button to have the ISG50 capture packets according to the settings configured in this screen. You can configure the ISG50 while a packet capture is in progress although you cannot modify the packet capture settings. The ISG50's throughput or performance may be affected while a packet capture is in progress. After the ISG50 finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

56.3.1 The Packet Capture Files Screen

Click **Maintenance > Diagnostics > Packet Capture > Files** to open the packet capture files screen. This screen lists the files of packet captures stored on the ISG50 or a connected USB storage device. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 503 Maintenance > Diagnostics > Packet Capture > Files


Diagnostics
Packet Capture
Core Dump
System Log
Capture
Files
Captured Packet Files
Remove
Download
Page 1 of 1
Show 50 items
Displaying 1 - 2 of 2
Captured Packet Files in USB storage
Remove
Download
Page 1 of 1
Show 50 items
No data to display

#	File Name	Size	Last Modified
1	wan1--packet-capture.00000.cap	367548	2010-11-24 01:50:31
2	wan1--packet-capture.txt	81	2010-11-24 01:50:31

The following table describes the labels in this screen.

Table 297 Maintenance > Diagnostics > Packet Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ISG50 or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.

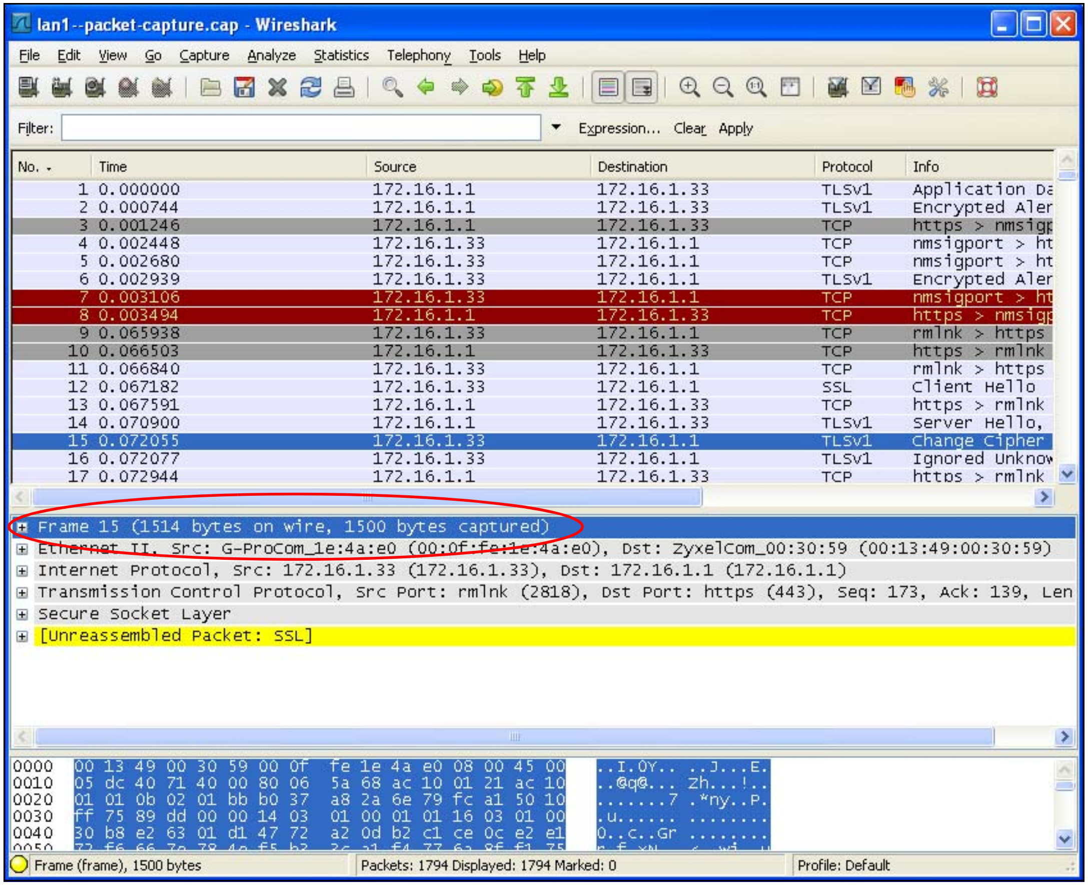
Table 297 Maintenance > Diagnostics > Packet Capture > Files (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

56.3.2 Example of Viewing a Packet Capture File

Here is an example of a packet capture file viewed in the Wireshark packet analyzer. Notice that the size of frame 15 on the wire is 1514 bytes while the captured size is only 1500 bytes. The ISG50 truncated the frame because the capture screen's **Number Of Bytes To Capture (Per Packet)** field was set to 1500 bytes.

Figure 504 Packet Capture File Example



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	172.16.1.33	TLSv1	Application Da
2	0.000744	172.16.1.1	172.16.1.33	TLSv1	Encrypted Aler
3	0.001246	172.16.1.1	172.16.1.33	TCP	https > nmsigp
4	0.002448	172.16.1.33	172.16.1.1	TCP	nmsigport > ht
5	0.002680	172.16.1.33	172.16.1.1	TCP	nmsigport > ht
6	0.002939	172.16.1.33	172.16.1.1	TLSv1	Encrypted Aler
7	0.003106	172.16.1.33	172.16.1.1	TCP	nmsigport > ht
8	0.003494	172.16.1.1	172.16.1.33	TCP	https > nmsigp
9	0.065938	172.16.1.33	172.16.1.1	TCP	rmlnk > https
10	0.066503	172.16.1.1	172.16.1.33	TCP	https > rmlnk
11	0.066840	172.16.1.33	172.16.1.1	TCP	rmlnk > https
12	0.067182	172.16.1.33	172.16.1.1	SSL	Client Hello
13	0.067591	172.16.1.1	172.16.1.33	TCP	https > rmlnk
14	0.070900	172.16.1.1	172.16.1.33	TLSv1	Server Hello,
15	0.072055	172.16.1.33	172.16.1.1	TLSv1	Change Cipher
16	0.072077	172.16.1.33	172.16.1.1	TLSv1	Ignored Unknow
17	0.072944	172.16.1.1	172.16.1.33	TCP	https > rmlnk

```
⊞ Frame 15 (1514 bytes on wire, 1500 bytes captured)
⊞ Ethernet II, Src: G-ProCom_1e:4a:e0 (00:0f:fe:1e:4a:e0), Dst: ZyxelCom_00:30:59 (00:13:49:00:30:59)
⊞ Internet Protocol, Src: 172.16.1.33 (172.16.1.33), Dst: 172.16.1.1 (172.16.1.1)
⊞ Transmission Control Protocol, Src Port: rmlnk (2818), Dst Port: https (443), Seq: 173, Ack: 139, Len
⊞ Secure Socket Layer
⊞ [Unreassembled Packet: SSL]
```

```
0000  00 13 49 00 30 59 00 0f  fe 1e 4a e0 08 00 45 00   ..I.0Y.. ..J...E.
0010  05 dc 40 71 40 00 80 06  5a 68 ac 10 01 21 ac 10   ..@q@... Zh...!..
0020  01 01 0b 02 01 bb b0 37  a8 2a 6e 79 fc a1 50 10   .......7 .*ny..P.
0030  ff 75 89 dd 00 00 14 03  01 00 01 01 16 03 01 00   .u...... ........
0040  30 b8 e2 63 01 d1 47 72  a2 0d b2 c1 ce 0c e2 e1   0..c..Gr ........
```

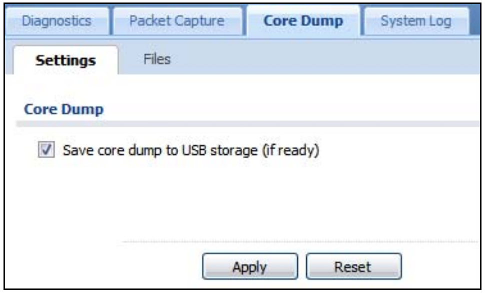
Frame (frame), 1500 bytes | Packets: 1794 Displayed: 1794 Marked: 0 | Profile: Default

56.4 Core Dump Screen

Use the **Core Dump** screen to have the ISG50 save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.

Click **Maintenance > Diagnostics > Core Dump** to open the following screen.

Figure 505 Maintenance > Diagnostics > Core Dump


Diagnostics
Packet Capture
Core Dump
System Log
Settings
Files
Core Dump
Apply
Reset

☑ Save core dump to USB storage (if ready)

The following table describes the labels in this screen.

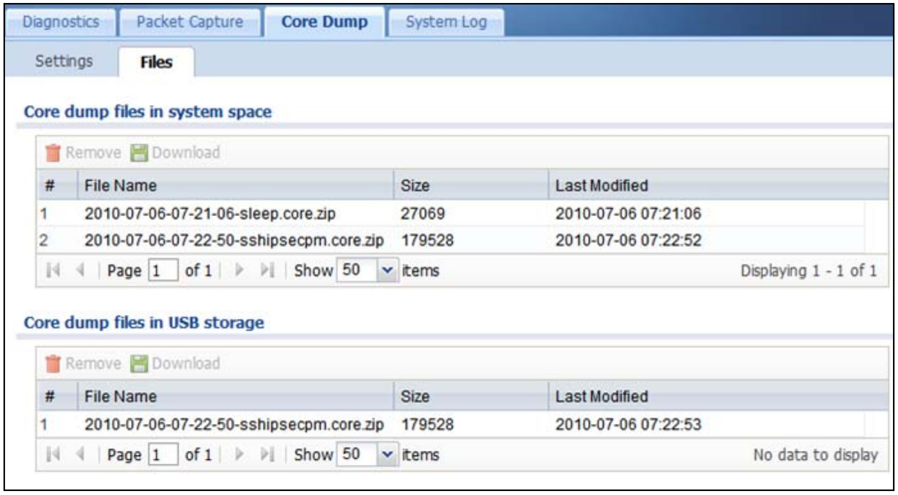
Table 298 Maintenance > Diagnostics > Core Dump

LABEL	DESCRIPTION
Save core dump to USB storage (if ready)	Select this to have the ISG50 save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). If you clear this option the ISG50 only saves
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

56.4.1 Core Dump Files Screen

Click **Maintenance > Diagnostics > Core Dump > Files** to open the core dump files screen. This screen lists the core dump files stored on the ISG50 or a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 506 Maintenance > Diagnostics > Core Dump > Files


Diagnostics
Packet Capture
Core Dump
System Log
Settings
Files
Remove
Download
Page 1 of 1
Show 50 items
Remove
Download
Page 1 of 1
Show 50 items

Core dump files in system space

#	File Name	Size	Last Modified
1	2010-07-06-07-21-06-sleep.core.zip	27069	2010-07-06 07:21:06
2	2010-07-06-07-22-50-sshipsecpm.core.zip	179528	2010-07-06 07:22:52

Displaying 1 - 1 of 1

Core dump files in USB storage

#	File Name	Size	Last Modified
1	2010-07-06-07-22-50-sshipsecpm.core.zip	179528	2010-07-06 07:22:53

No data to display

The following table describes the labels in this screen.

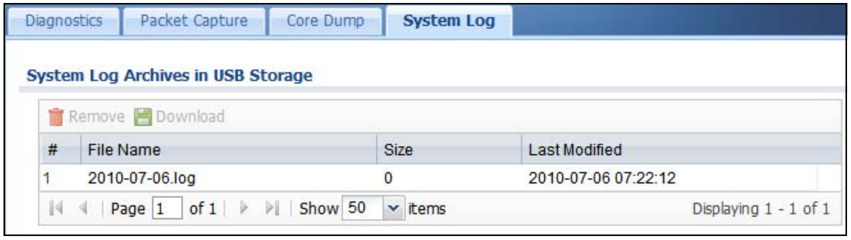
Table 299 Maintenance > Diagnostics > Core Dump > Files

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ISG50. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

56.5 The System Log Screen

Click **Maintenance > Diagnostics > System Log** to open the system log files screen. This screen lists the files of system logs stored on a connected USB storage device. The files are in comma separated value (CSV) format. You can download them to your computer and open them in a tool like Microsoft's Excel.

Figure 507 Maintenance > Diagnostics > System Log



#	File Name	Size	Last Modified
1	2010-07-06.log	0	2010-07-06 07:22:12

The following table describes the labels in this screen.

Table 300 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ISG50. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

57

Packet Flow Explore

57.1 Overview

Use this to get a clear picture on how the ISG50 determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot any related problems.

57.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen (see Section 57.2 on page 745) to view the overall routing flow and each routing function's settings.
- Use the **SNAT Status** screen (see Section 57.3 on page 750) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

57.2 The Routing Status Screen

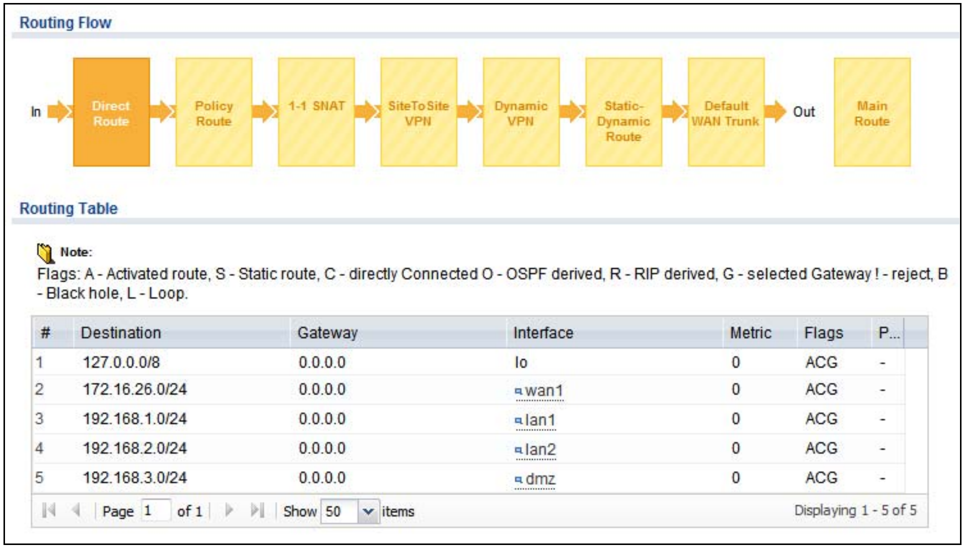
The **Routing Status** screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the **Routing Flow** section, the related routes (activated) will display in the **Routing Table** section. To access this screen, click **Maintenance** > **Packet Flow Explore**.

The order of the routing flow may vary depending on whether you:

- select **use policy route to override direct route** in the **CONFIGURATION > Network > Routing > Policy Route** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.
- select **use policy routes to control dynamic IPSec rules** in the **CONFIGURATION > VPN > IPSec VPN > VPN Connection** screen.

Note: Once a packet matches the criteria of a routing rule, the ISG50 takes the corresponding action and does not perform any further flow checking.

Figure 508 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

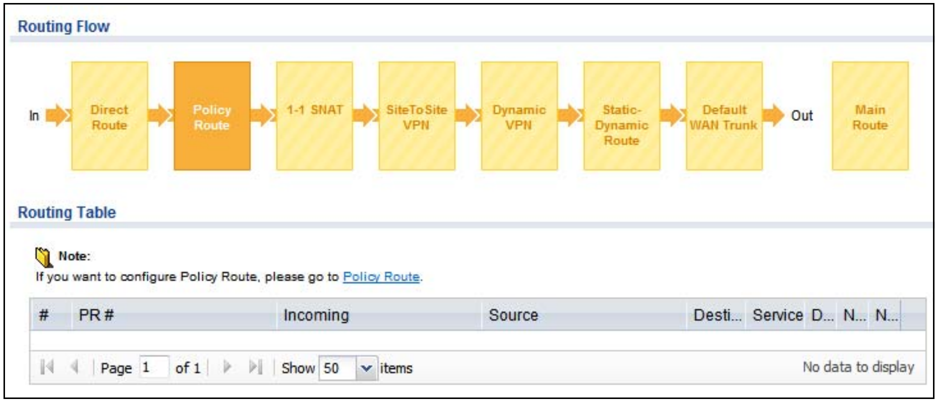

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, G - selected Gateway ! - reject, B - Black hole, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	P...
1	127.0.0.0/8	0.0.0.0	lo	0	ACG	-
2	172.16.26.0/24	0.0.0.0	wan1	0	ACG	-
3	192.168.1.0/24	0.0.0.0	lan1	0	ACG	-
4	192.168.2.0/24	0.0.0.0	lan2	0	ACG	-
5	192.168.3.0/24	0.0.0.0	dmz	0	ACG	-

Page 1 of 1
Show 50 items
Displaying 1 - 5 of 5

Figure 509 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

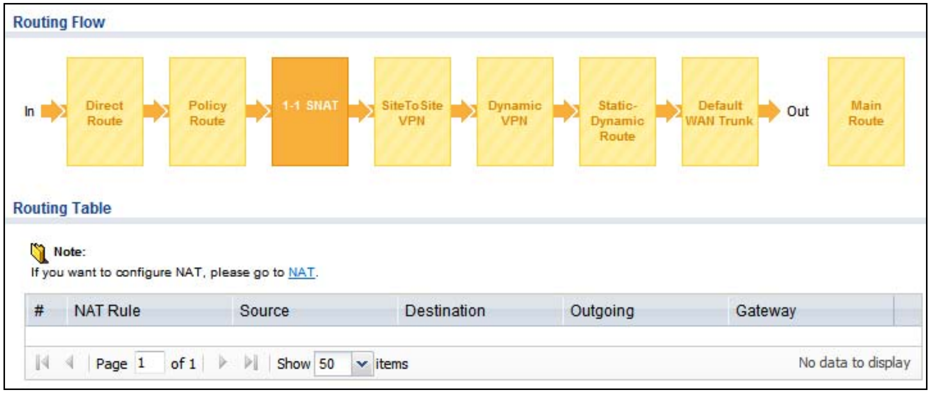

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
If you want to configure Policy Route, please go to Policy Route.

#	PR #	Incoming	Source	Desti...	Service	D...	N...	N...

Page 1 of 1
Show 50 items
No data to display

Figure 510 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

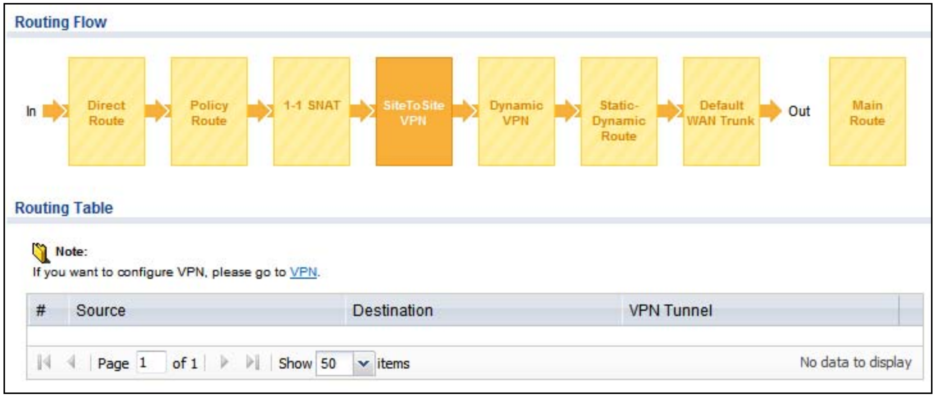

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
If you want to configure NAT, please go to NAT.

#	NAT Rule	Source	Destination	Outgoing	Gateway

Page 1 of 1
Show 50 items
No data to display

Figure 511 Maintenance > Packet Flow Explore > Routing Status (SitetoSite VPN)

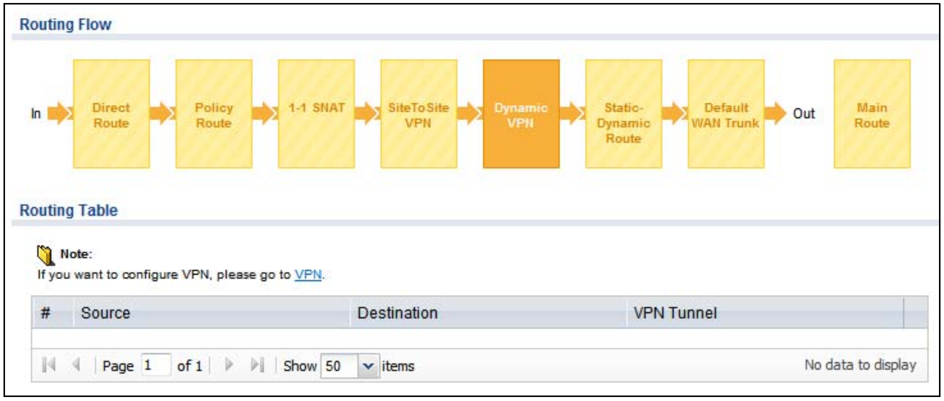

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
If you want to configure VPN, please go to VPN.

#	Source	Destination	VPN Tunnel

Page 1 of 1 Show 50 items No data to display

Figure 512 Maintenance > Packet Flow Explore > Routing Status (Dynamic VPN)

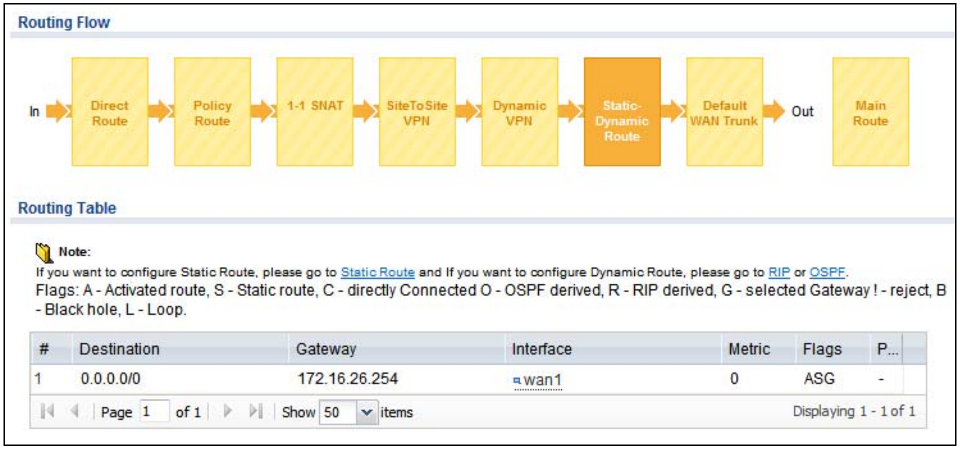

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
If you want to configure VPN, please go to VPN.

#	Source	Destination	VPN Tunnel

Page 1 of 1 Show 50 items No data to display

Figure 513 Maintenance > Packet Flow Explore > Routing Status (Static-Dynamic Route)

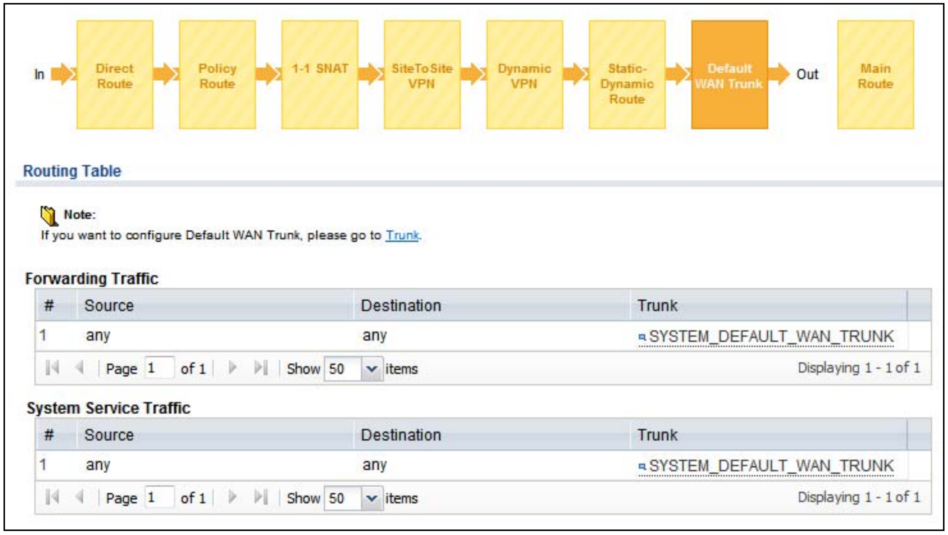

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
If you want to configure Static Route, please go to Static Route and If you want to configure Dynamic Route, please go to RIP or OSPF.
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, G - selected Gateway ! - reject, B - Black hole, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	P...
1	0.0.0.0/0	172.16.26.254	wan1	0	ASG	-

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Figure 514 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)


In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
If you want to configure Default WAN Trunk, please go to Trunk.

Forwarding Traffic

#	Source	Destination	Trunk
1	any	any	SYSTEM_DEFAULT_WAN_TRUNK

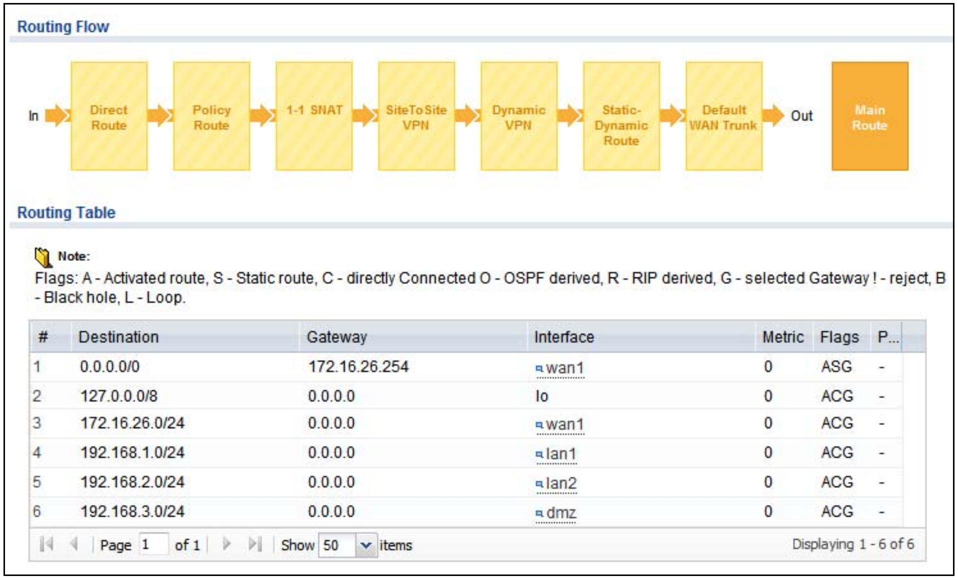
Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

System Service Traffic

#	Source	Destination	Trunk
1	any	any	SYSTEM_DEFAULT_WAN_TRUNK

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Figure 515 Maintenance > Packet Flow Explore > Routing Status (Main Route)


Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Out
Main Route
Routing Table

Note:
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, G - selected Gateway ! - reject, B - Black hole, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	P...
1	0.0.0.0/0	172.16.26.254	wan1	0	ASG	-
2	127.0.0.0/8	0.0.0.0	lo	0	ACG	-
3	172.16.26.0/24	0.0.0.0	wan1	0	ACG	-
4	192.168.1.0/24	0.0.0.0	lan1	0	ACG	-
5	192.168.2.0/24	0.0.0.0	lan2	0	ACG	-
6	192.168.3.0/24	0.0.0.0	dmz	0	ACG	-

Page 1 of 1 | Show 50 items | Displaying 1 - 6 of 6

The following table describes the labels in this screen.

Table 301 Maintenance > Packet Flow Explore > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the ISG50 determines where to route a packet. Click a function box to display the related settings in the **Routing Table** section.
Routing Table	This section shows the corresponding settings according to the function box you click in the **Routing Flow** section.
The following fields are available if you click **Direct Route**, **Static-Dynamic Route**, or **Main Route** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Gateway	This is the IP address of the next-hop gateway or the interface through which the traffic is routed.
Interface	This is the name of an interface associated with the route.

Table 301 Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
Metric	This is the route’s priority among the displayed routes.
Flags	This indicates additional information for the route. The possible flags are: • **A** - this route is currently activated • **S** - this is a static route • **C** - this is a direct connected route • **O** - this is a dynamic route learned through OSPF • **R** - this is a dynamic route learned through RIP • **G** - the route is to a gateway (router) in the same network. • **!** - this is a route which forces a route lookup to fail. • **B** - this is a route which discards packets. • **L** - this is a recursive route.
Persist	This is the remaining time of a dynamically learned route. The ISG50 removes the route after this time period is counted down to zero.
The following fields are available if you click **Policy Route** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route. If you have configured a schedule for the route, this screen only displays the route at the scheduled time.
Incoming	This is the interface on which the packets are received.
Source	This is the source IP address(es) from which the packets are sent.
Destination	This is the destination IP address(es) to which the packets are transmitted.
Service	This is the name of the service object. **any** means all services.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. See Section 14.2 on page 291 for more information.
Next Hop Type	This is the type of the next hop to which packets are directed.
Next Hop Info	• This is the main route if the next hop type is **Auto**. • This is the interface name and gateway IP address if the next hop type is **Interface / GW**. • This is the tunnel name if the next hop type is **VPN Tunnel**. • This is the trunk name if the next hop type is **Trunk**.
The following fields are available if you click **1-1 SNAT** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.
Source	This is the original source IP address(es). **any** means any IP address.
Destination	This is the original destination IP address(es). **any** means any IP address.
Outgoing	This is the name of an interface which transmits packets out of the ISG50.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click **SiteToSite VPN** or **Dynamic VPN** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the IP address(es) of the local VPN network.
Destination	This is the IP address(es) for the remote VPN network.
VPN Tunnel	This is the name of the VPN tunnel.
The following fields are available if you click **Default WAN Trunk** in the **Routing Flow** section.	
Forwarding Traffic	This section displays information about traffic going through the ISG50.

Table 301 Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
System Service Traffic	This section displays information about traffic originating from the ISG50 itself.
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the source IP address(es) from which the packets are sent. **any** means any IP address.
Destination	This is the destination IP address(es) to which the packets are transmitted. **any** means any IP address.
Trunk	This is the name of the WAN trunk through which the matched packets are transmitted.

57.3 The SNAT Status Screen

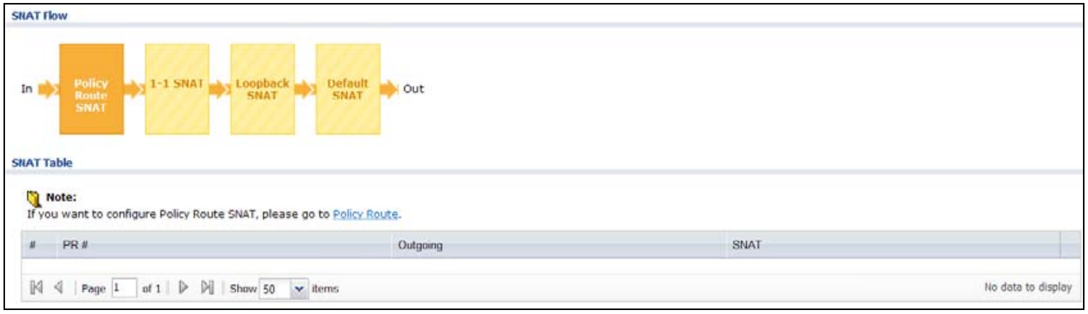
The **SNAT Status** screen allows you to view and quickly link to specific source NAT (SNAT) settings. Click a function box in the **SNAT Flow** section, the related SNAT rules (activated) will display in the **SNAT Table** section. To access this screen, click **Maintenance** > **Packet Flow Explore** > **SNAT Status**.

The order of the SNAT flow may vary depending on whether you:

- select **use default SNAT** in the **CONFIGURATION > Network > Interface > Trunk** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.

Note: Once a packet matches the criteria of an SNAT rule, the ISG50 takes the corresponding action and does not perform any further flow checking.

Figure 516 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

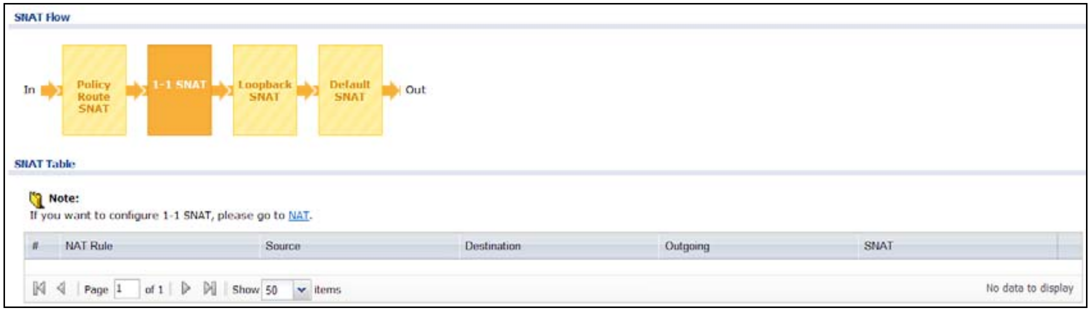

SNAT Flow
In
Policy Route SNAT
1-1 SNAT
Loopback SNAT
Default SNAT
Out
SNAT Table

Note:
If you want to configure Policy Route SNAT, please go to Policy Route.

#	PR #	Outgoing	SNAT

Page 1 of 1
Show 50 items
No data to display

Figure 517 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

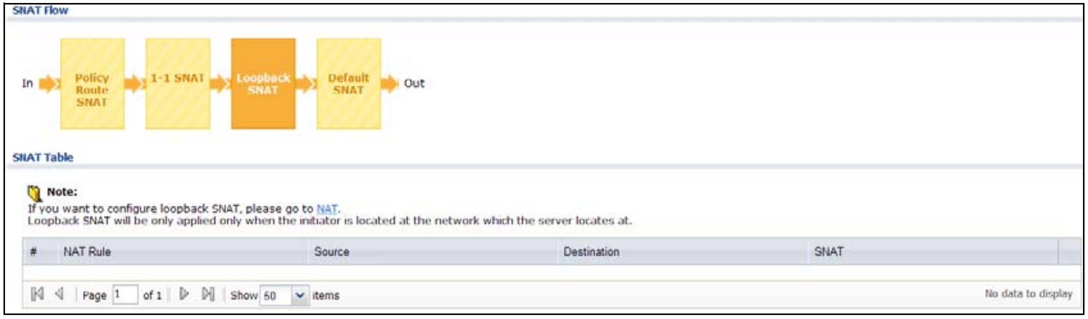

SNAT Flow
In
Policy Route SNAT
1-1 SNAT
Loopback SNAT
Default SNAT
Out
SNAT Table

Note:
If you want to configure 1-1 SNAT, please go to NAT.

#	NAT Rule	Source	Destination	Outgoing	SNAT

Page 1 of 1
Show 50 items
No data to display

Figure 518 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

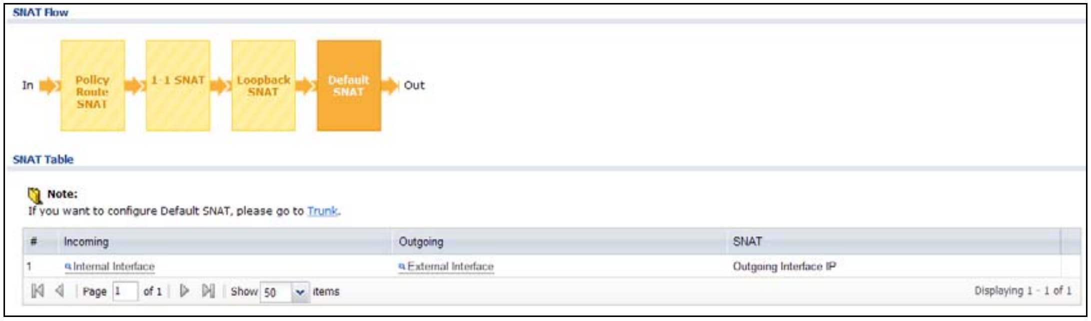

SNAT Flow
In
Policy Route SNAT
1-1 SNAT
Loopback SNAT
Default SNAT
Out
SNAT Table

Note:
If you want to configure loopback SNAT, please go to NAT.
Loopback SNAT will be only applied only when the initiator is located at the network which the server locates at.

#	NAT Rule	Source	Destination	SNAT

Page 1 of 1
Show 50 items
No data to display

Figure 519 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)


SNAT Flow
In
Policy Route SNAT
1-1 SNAT
Loopback SNAT
Default SNAT
Out
SNAT Table

Note:
If you want to configure Default SNAT, please go to Trunk.

#	Incoming	Outgoing	SNAT
1	Internal Interface	External Interface	Outgoing Interface IP

Page 1 of 1
Show 50 items
Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 302 Maintenance > Packet Flow Explore > SNAT Status

LABEL	DESCRIPTION
SNAT Flow	This section shows you the flow of how the ISG50 changes the source IP address for a packet according to the rules you have configured in the ISG50. Click a function box to display the related settings in the **SNAT Table** section.
SNAT Table	The table fields in this section vary depending on the function box you select in the **SNAT Flow** section.
The following fields are available if you click **Policy Route SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route which uses SNAT.
Outgoing	This is the outgoing interface that the route uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click **1-1 SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.
Source	This is the original source IP address(es).
Destination	This is the original destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click **Loopback SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.
Source	This is the original source IP address(es). **any** means any IP address.
Destination	This is the original destination IP address(es). **any** means any IP address.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, **Outgoing Interface IP** means that the ISG50 uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.
The following fields are available if you click **Default SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This indicates internal interface(s) on which the packets are received.
Outgoing	This indicates external interface(s) from which the packets are transmitted.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, **Outgoing Interface IP** means that the ISG50 uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.

58

Reboot

58.1 Overview

Use this to restart the device (for example, if the device begins behaving erratically). See also Section 1.7 on page 35 for information on different ways to start and stop the ISG50.

58.1.1 What You Need To Know

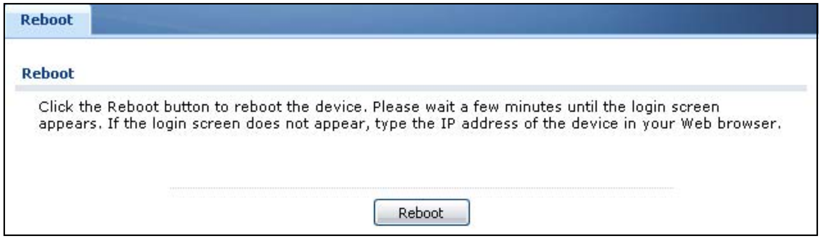
If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see Section 61.1 on page 774) reset returns the device to its default configuration.

58.2 The Reboot Screen

The **Reboot** screen is part of the Web configurator so that remote users can restart the device. To access this screen, click **Maintenance** > **Reboot**.

Figure 520 Maintenance > Reboot



Click the Reboot button to reboot the device. Please wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

Click the **Reboot** button to restart the ISG50. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the ISG50.

Shutdown

59.1 Overview

Use this to shutdown the device in preparation for disconnecting the power. See also Section 1.7 on page 35 for information on different ways to start and stop the ISG50.

Always use the Maintenance > Shutdown > Shutdown screen or the “shutdown” command before you turn off the ISG50 or remove the power. Not doing so can cause the firmware to become corrupt.

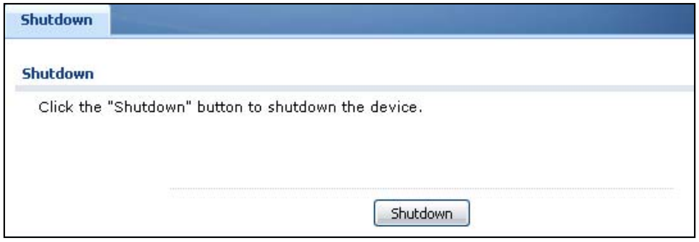
59.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

59.2 The Shutdown Screen

To access this screen, click **Maintenance** > **Shutdown**.

Figure 521 Maintenance > Shutdown



Click the "Shutdown" button to shutdown the device.

Click the **Shutdown** button to shut down the ISG50. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command `shutdown` to shutdown the ISG50.

60

Extension Portal

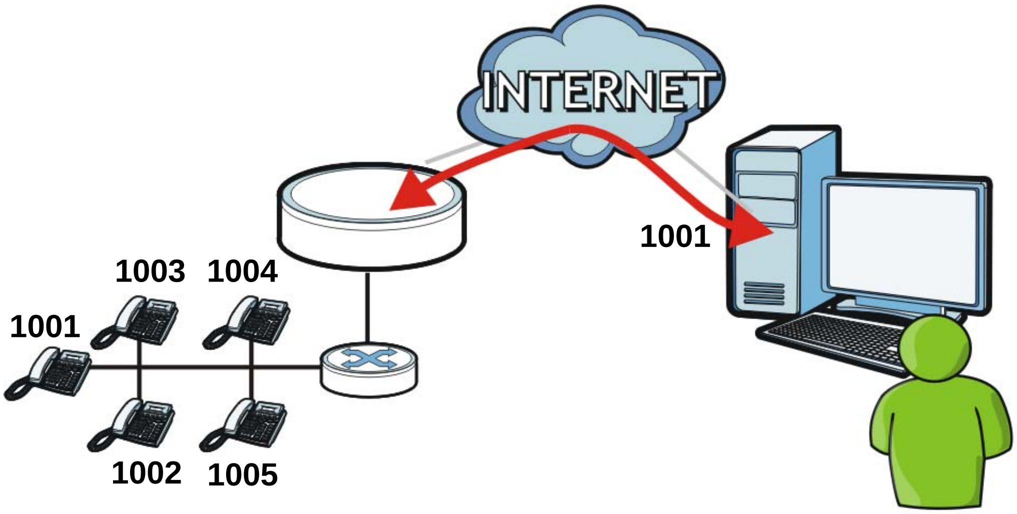
60.1 Overview

Use the extension portal to make calls via the web phone and manage settings for individual users.

The extension portal is a HTML-based phone as well as a management tool that allows users to manage some of the settings related to their telephone extension. Each extension created on the ISG50 has an associated account which allows it to log into the extension portal. When you login to the extension portal you can pick up and make calls using your browser.

The extension portal can be used by members of your organization who are working away from the office. As long as they have a reliable Internet connection, they can login to the extension portal and answer and make calls from the same extension as they have in the office. For example, a user working from home, can log into the extension portal with his desk phone extension (1001) and use the HTML-based phone to call extension 1002. He can also receive calls directed to extension 1001.

Figure 522 Extension Portal Overview



60.1.1 What You Can Do in this Chapter

- Use the **Web Phone** screen to make a call from the web phone. See Section 60.2 on page 759.
- Use the **Peer Info** screen to manage the passwords associated with your extension. See Section 60.3 on page 760.
- Use the **Call Forwarding and Blocking** screen to configure call forwarding and call blocking rules for your extension. See Section 60.4 on page 761.
- Use the **Voice Mail Settings** screen to set up the voice mail settings for your extension. See Section 60.5 on page 763.

- Use the **Call Recording** screen to play back calls you recorded on your extension. See Section 60.6 on page 764

60.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

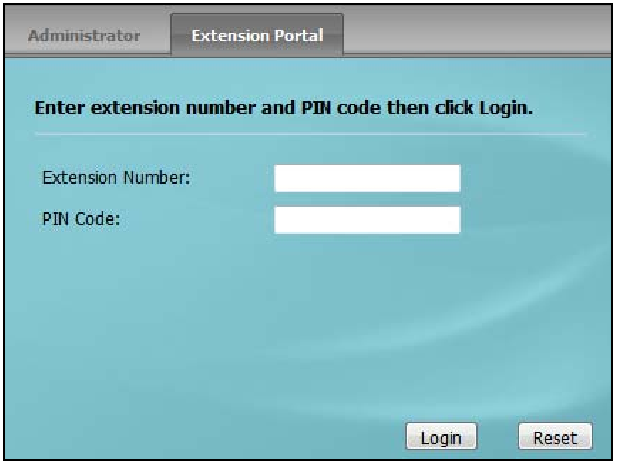
Extension Portal Login

1 Open Internet Explorer (the extension portal supports Internet Explorer).

2 Type “https://” and the IP address of the ISG50 (for example, the default LAN IP address is 192.168.1.1) in the **Location** or **Address** field. Press [ENTER]. To protect against brute force, password-guessing attacks, the ISG50 blocks an account’s access for 60 minutes after 3 consecutive, failed login attempts. You can use the commands to change this.

3 Continue past any warning messages to the **Login** screen. Click the **Extension Portal** tab.

Figure 523 Extension Portal Log In


Administrator
Extension Portal
Extension Number:
PIN Code:
Login
Reset

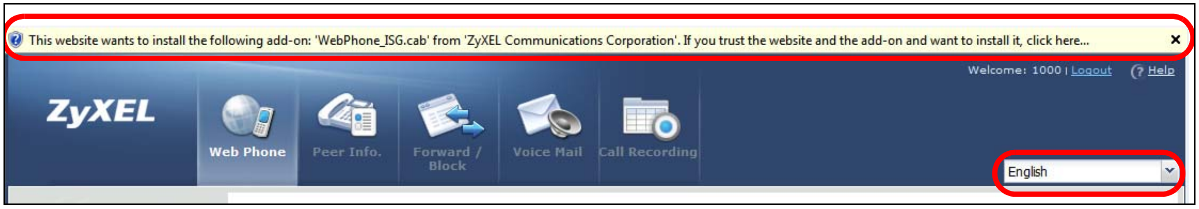
Enter extension number and PIN code then click Login.

4 Enter your extension number and the associated web password in the upper part of the login screen and click **Login**.

Note: The web password is set up by the administrator when the extension is initially created. See Chapter 29 on page 453.

5 Click the message at the top of the screen to have Internet Explorer install the web phone add-on. Then select your language.

Figure 524 Web Phone Add-on Install and Language Selection

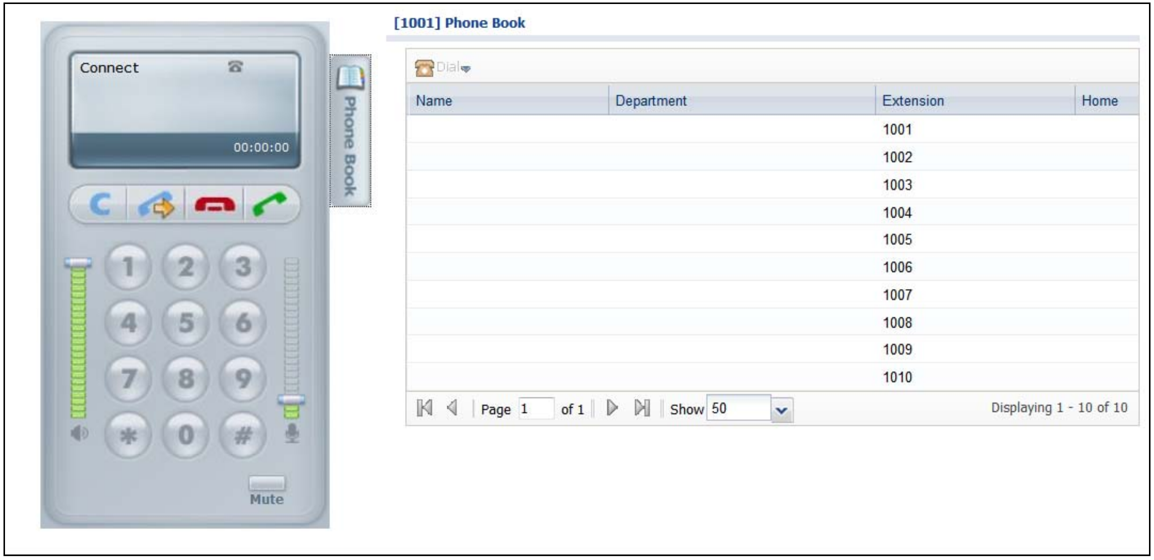

Welcome: 1000 | Logout
Help
ZyXEL
Web Phone
Peer Info.
Forward / Block
Voice Mail
Call Recording
English

This website wants to install the following add-on: 'WebPhone_ISG.cab' from 'ZyXEL Communications Corporation'. If you trust the website and the add-on and want to install it, click here...

60.2 Web Phone

Use this screen to make calls from the web phone. To access this screen, click the **Web Phone** tab in the extension portal.

Figure 525 Web Phone



Name	Department	Extension	Home
		1001	
		1002	
		1003	
		1004	
		1005	
		1006	
		1007	
		1008	
		1009	
		1010	

Each field is described in the following table.

Table 303 Web Phone

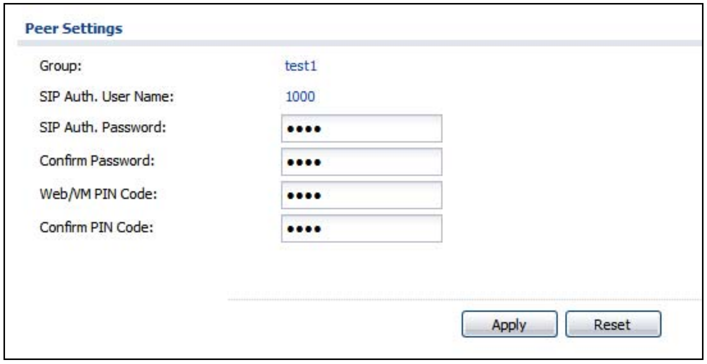
LABEL	DESCRIPTION
Phone Book	Click the **Phone Book** tab on the right side of the **Web Phone** screen to display or hide the phone book feature. Use the the phone book
Call Duration	This total time of your conversation is displayed above the input field in the web phone GUI.
Input Text	Type or use your keypad to enter the phone number you want to dial. The web phone follows the same dialing rules that you have to follow when you are making calls from any other phone connected to the ISG50.
Status	The status of your phone call is displayed below the text input field. The web phone GUI displays the current status of a phone call, that is "Ringing", "Talking" or "Bye". It also displays the phone number you dialed from the web phone.
Phone Keypad	You can use your mouse to click on the numbers that make up the telephone number you want to dial. Use the **Clear** icon (C) to delete digits from the screen. Use the **Dial/Pick up** icon (☎) to dial the number. Use the **Hang up** icon (☎) to end a call or to delete a number in the input field. Use the **Transfer** icon (⇨) to forward a call to another extension.

60.3 Peer Info

Use this screen to manage the passwords associated with your extension. To access this screen, click **Peer info.**

Note: Some of the fields are not applicable for FXS extensions and do not display when analog phone users log into the personal extension portal.

Figure 526 Peer Info



Peer Settings

Group: test1

SIP Auth. User Name: 1000

SIP Auth. Password: ••••

Confirm Password: ••••

Web/VM PIN Code: ••••

Confirm PIN Code: ••••

Each field is described in the following table.

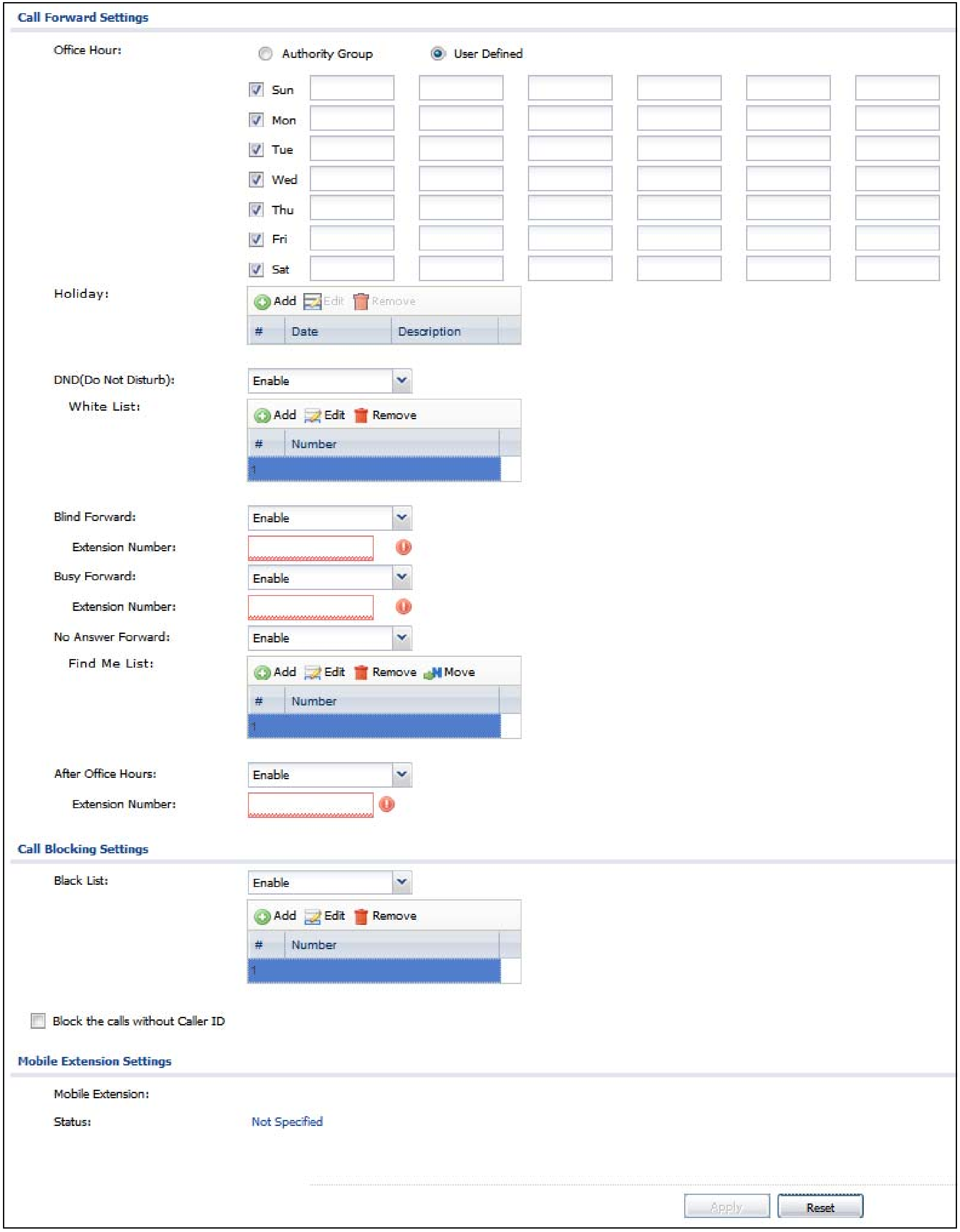
Table 304 Peer Info

LABEL	DESCRIPTION
Group	This is a read-only field showing the authority group this extension belongs to.
SIP Auth. User Name	This is a read-only field showing the SIP user name associated with this extension. This field is not available for FXS and BRI extensions on the ISG50.
SIP Auth. Password	Use these fields to change the SIP password associated with this extension. Type and retype the new password for this extension. This is the password you will need to enter when registering a SIP phone with the ISG50. This field is not available for FXS and BRI extensions on the ISG50.
Web/VM PIN Code	Use these fields to change the PIN (Personal Identification Number) you need to enter when accessing the extension portal or voice mail. Type the new PIN.
Confirm PIN Code	Retype the new PIN for confirmation.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to begin configuring the fields again.

60.4 Call Forwarding and Blocking

Use this screen to set up call forwarding and call blocking rules for your extension. To access this screen, click **Forward/Block** in the extension portal.

Figure 527 Forward/Block



Call Forward Settings

Office Hour: ○ Authority Group ● User Defined

☑ Sun
☑ Mon
☑ Tue
☑ Wed
☑ Thu
☑ Fri
☑ Sat

Holiday:

#	Date	Description

DND(Do Not Disturb): Enable

White List:

#	Number
1	

Blind Forward: Enable

Extension Number:

Busy Forward: Enable

Extension Number:

No Answer Forward: Enable

Find Me List:

#	Number
1	

After Office Hours: Enable

Extension Number:

Call Blocking Settings

Black List: Enable

#	Number
1	

☐ Block the calls without Caller ID

Mobile Extension Settings

Mobile Extension:

Status: Not Specified

Each field is described in the following table.

Table 305 Forward/Block

LABEL	DESCRIPTION
Call Forward Settings	Use this section to configure call forwarding settings for your extension.
Office Hour	The ISG50 has separate rules for call forwarding during office hours than after office hours. For information, see Chapter 43 on page 595. Select **Authority Group** to have the extension use the office hours defined for the authority group to which it belongs. Select **User Defined** to specify custom office hours for this extension.
Sun ~ Sat	Select the days of the week which you want the ISG50 to treat as working days. Specify the time range during the working days that you want the ISG50 to treat as working hours. When entering a time range, the following conditions apply: • You can enter up to six time ranges, with each range consisting of a start time and an end time. • The time entered in each field must be in 24 hour format (such as “08:00” for 8 AM or “13:00” for 1 PM). • The start and end times must be separated by a hyphen.
Holiday	This section allows you to set a specific day of the year as a holiday, which the ISG50 will then treat as “after office hours”.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to modify it.
Remove	To remove an entry, select it and click **Remove**. The ISG50 confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Date	Enter a date in mm/dd format (double digit month / day; for example, 02/09 for February 9th.)
Description	Enter a description of the holiday using up to 63 alphanumeric characters (A-Z, a-z, 0-9) and spaces.
DND (Do Not Disturb)	Select **Disable** to turn this feature off for this extension. Select **Enable** and the ISG50 will not forward calls to your extension. Use the **White List** to configure telephone numbers which ignore whether you have DND turned on or off. Use the **Add**, **Edit**, and **Remove** icons to create, modify, or delete entries. Select **Voice Mail** and the ISG50 will forward calls directly to voice mail.
Blind Forward	Select **Disable** to turn this feature off for this extension. Select **Enable** and specify an extension or other phone number 3-20 digits in length. The ISG50 will forward all incoming calls to that extension. Select **Voice Mail** and the ISG50 will forward calls directly to voice mail.
Busy Forward	Select **Disable** to turn this feature off for this extension. Select **Enable** and specify an extension or other phone number 3-20 digits in length to forward all incoming calls to that extension when the phone is off the hook. For FXS (analog phones) extensions incoming calls are put into a call waiting queue. Select **Voice Mail** to forward calls directly to voice mail.

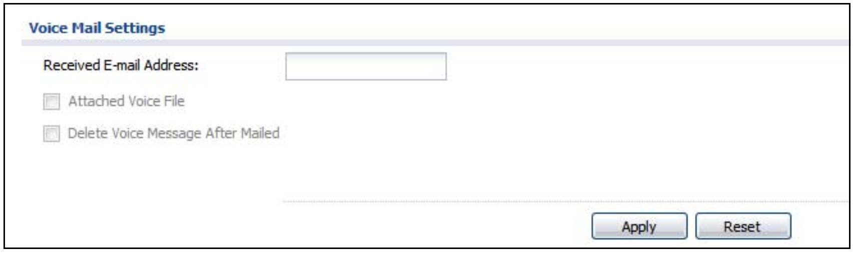
Table 305 Forward/Block (continued)

LABEL	DESCRIPTION
No Answer Forward	Select **Disable** to turn this feature off for this extension. Select **Enable** to forward all incoming calls to the extensions specified in the **Find Me List** when this extension is not answered within the default ring time. Use the **Add**, **Edit**, and **Remove** icons to create, modify, or delete **Find Me List** entries. Select **Voice Mail** to forward calls directly to voice mail.
After Office Hours	These fields specify how to treat calls to your extension that occur after office hours. Select **Disable** to turn this feature off for this extension. Select **Enable** and specify an extension or other phone number 3-20 digits in length. The ISG50 will forward all incoming calls to that extension. Select **Voice Mail** to forward calls directly to voice mail.
Call Blocking Setting	Use this section to configure call blocking settings for your extension.
Black List	Select **Disable** to turn this feature off for this extension. Select **Enable** and the ISG50 will block all incoming calls from extensions that you specify as blacklisted. Use the **Black List** to configure phone numbers that you want to block from calling you. Use the **Add**, **Edit**, and **Remove** icons to create, modify, or delete entries.
Block the calls without Caller ID	Select **Enable** and the ISG50 will block all incoming calls from phone that do not send caller ID.
Mobile Extension Setting	This section displays information about your mobile extension, if one has been configured for you. For more information on this, see Chapter 29 on page 453.
Mobile Extension	This displays the phone number to which all calls sent to your extension will be forwarded.
Status	This indicates your mobile extension feature is on, off, or not enabled.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to begin configuring the fields again.

60.5 Voice Mail Settings

Use this screen to set up the voice mail settings for your extension. To access this screen, click the **Voice Mail** tab in the extension portal.

Figure 528 Voice Mail



Each field is described in the following table.

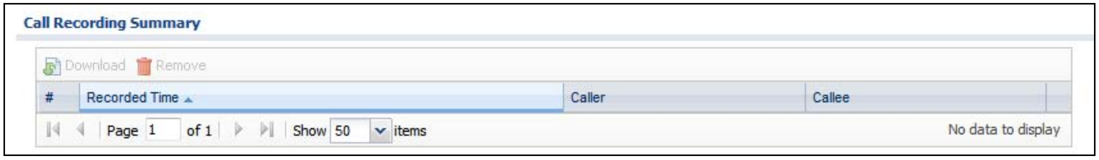
Table 306 Voice Mail

LABEL	DESCRIPTION
Received E-mail Address	Specify the e-mail address you want to forward your voice message notifications to. If you select the **Attached Voice File** option, then complete voice messages are sent to this e-mail address.
Attached Voice File	Select this feature if you want complete voice messages to be sent to the e-mail address you specified in the **Received E-mail Address** field.
Delete Voice Mail After Mailed	Check this box to delete voicemail messages stored on the ISG50 after they have been e-mailed.
Apply	Click this to save your changes and to apply them to the ISG50.
Reset	Click this to begin configuring the fields again.

60.6 Call Recording

Use this screen to play back calls you recorded on your extension. To access this screen, click the **Call Recording** tab in the extension portal.

Figure 529 Call Recording



Each field is described in the following table.

Table 307 Call Recording

LABEL	DESCRIPTION
Download	Select an entry and click **Download** to save the call recording to your computer.
Remove	Select an entry or entries and click **Remove** to delete them from the ISG50. Note: Only recordings triggered by the on-demand recording by this extension can be removed here.
#	This is the number of the entry in the list.
Recorded Time	This is the time that the call recording started. Click an entry to play the call recording.
Caller	This is the number that initiated the call. This cell is highlighted if the number is for a peer in the recording list.
Callee	This is the number that received the call. This cell is highlighted if the number is for a peer in the recording list.

61

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Chapter 10 on page 220). For individual log descriptions, see the User's Guide appendix Appendix A on page 775.
- For the order in which the ISG50 applies its features and checks, see Section 6.5 on page 94.

None of the LEDs turn on.

Make sure that you have the power cord connected to the ISG50 and plugged in to an appropriate power source. Make sure you have the ISG50 turned on. Check all cable connections.

If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Cannot access the ISG50 from the LAN.

- Check the cable connection between the ISG50 and your computer or switch.
- Ping the ISG50 from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly. Also make sure that its IP address is in the same subnet as the ISG50's.
- In the computer, click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the ISG50's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The ISG50 should reply.
- If you've forgotten the ISG50's password, use the **RESET** button. Press the button in for about 5 seconds (or until the **PWR** LED starts to blink), then release it. It returns the ISG50 to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.; see your User's Guide for details).

- If you’ve forgotten the ISG50’s IP address, you can use the commands through the console port to check it. Connect your computer to the **CONSOLE** port using a console cable. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 115200 bps port speed.

I cannot access the Internet.

- Check the ISG50’s connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
- Check the WAN interface's status in the **Dashboard**. Use the installation setup wizard again and make sure that you enter the correct settings. Use the same case as provided by your ISP.

I cannot use the web phone.

- You must use Internet Explorer to use the extension portal and web phone.
- Your computer must also have a microphone and speakers connected and enabled.

I configured security settings but the ISG50 is not applying them for certain interfaces.

Many security settings are usually applied to zones. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

The ISG50 is not applying the custom policy route I configured.

The ISG50 checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that the traffic would also match.

The ISG50 is not applying the custom firewall rule I configured.

The ISG50 checks the firewall rules in the order that they are listed. So make sure that your custom firewall rule comes before any other rules that the traffic would also match.

I cannot enter the interface name I want.

- The format of interface names other than the Ethernet interface names is very strict. Each name consists of 2-4 letters (interface type), followed by a number (x, limited by the maximum number of each type of interface). For example, VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.
- The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

I cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface on an Ethernet interface.

You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

My rules and settings that apply to a particular interface no longer work.

The interface’s IP address may have changed. To avoid this create an IP address object based on the interface. This way the ISG50 automatically updates every rule or setting that uses the object whenever the interface’s IP address settings change. For example, if you change LAN1’s IP address, the ISG50 automatically updates the corresponding interface-based, LAN1 subnet address object.

I cannot set up a PPP interface.

You have to set up an ISP account before you create a PPPoE or PPTP interface.

The data rates through my cellular connection are no-where near the rates I expected.

The actual cellular data rate you obtain varies depending on the cellular device you use, the signal strength to the service provider’s base station, and so on.

I created a cellular interface but cannot connect through it.

- Make sure you have a compatible 3G device installed or connected. See www.zyxel.com for details.
- Make sure you have the cellular interface enabled.

- Make sure the cellular interface has the correct user name, password, and PIN code configured with the correct casing.
- If the ISG50 has multiple WAN interfaces, make sure their IP addresses are on different subnets.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured it on top of another Ethernet interface.

Each VLAN interface is created on top of only one Ethernet interface.

The ISG50 is not applying an interface's configured ingress bandwidth limit.

At the time of writing, the ISG50 does not support ingress bandwidth management.

The ISG50's performance seems slower after configuring ADP.

Depending on your network topology and traffic load, applying an anomaly profile to each and every packet direction may affect the ISG50's performance.

The ISG50 routes and applies SNAT for traffic from some interfaces but not from others.

The ISG50 automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic. You must manually configure a policy route to add routing and SNAT settings for an interface with the **Interface Type** set to **General**. You can also configure a policy route to override the default routing and SNAT behavior for an interface with the **Interface Type** set to **Internal** or **External**.

The ISG50 is not applying a policy route's port triggering settings.

You also need to create a firewall rule to allow an incoming service.

I cannot get Dynamic DNS to work.

- You must have a public WAN IP address to use Dynamic DNS.
- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the ISG50.

- You may need to configure the DDNS entry's IP Address setting to **Auto** if the interface has a dynamic IP address or there are one or more NAT routers between the ISG50 and the DDNS server.
- The ISG50 may not determine the proper IP address if there is an HTTP proxy server between the ISG50 and the DDNS server.

I cannot create a second HTTP redirect rule for an incoming interface.

You can configure up to one HTTP redirect rule for each (incoming) interface.

The ISG50 keeps resetting the connection.

If an alternate gateway on the LAN has an IP address in the same subnet as the ISG50's LAN IP address, return traffic may not go through the ISG50. This is called an asymmetrical or "triangle" route. This causes the ISG50 to reset the connection, as the connection has not been acknowledged.

You can set the ISG50's firewall to permit the use of asymmetrical route topology on the network (so it does not reset the connection) although this is not recommended since allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ISG50. A better solution is to use virtual interfaces to put the ISG50 and the backup gateway on separate subnets. See Asymmetrical Routes on page 360 and the chapter about interfaces for more information.

I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both ZyXEL IPSec routers and check the settings in each field methodically and slowly. Make sure both the ISG50 and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Chapter 24 on page 367.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPSec device must also have NAT traversal enabled.
- The ISG50 and remote IPSec router must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode.
- Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.
- When using manual keys, the ISG50 and remote IPSec router must use the same encryption key and authentication key.
- When using pre-shared keys, the ISG50 and the remote IPSec router must use the same pre-shared key.

- The ISG50's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.
- The ISG50 and remote IPSec router must use the same active protocol.
- The ISG50 and remote IPSec router must use the same encapsulation.
- The ISG50 and remote IPSec router must use the same SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the ISG50 and remote IPSec router (for example, by using a packet sniffer).

Check the configuration for the following ISG50 features.

- The ISG50 does not put IPSec SAs in the routing table. You must create a policy route for each VPN tunnel. See Chapter 14 on page 289.
- Make sure the To-ISG50 firewall rules allow IPSec VPN traffic to the ISG50. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The ISG50 supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-ISG50 firewall rules allow UDP port 4500 too.
- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the ISG50 sends before the ISG50 encrypts them and check packets the ISG50 receives after the ISG50 decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the ISG50 and remote IPSec router use certificates to authenticate each other, You must set up the certificates for the ISG50 and remote IPSec router first and make sure they trust each other's certificates. If the ISG50's certificate is self-signed, import it into the remote IPsec router. If it is signed by a CA, make sure the remote IPsec router trusts that CA. The ISG50 uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
- Multiple SAs connecting through a secure gateway must have the same negotiation mode.

The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

If you have the **Configuration > VPN > IPSec VPN > VPN Connection** screen's **Use Policy Route to control dynamic IPSec rules option** enabled, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

I changed the LAN IP address and can no longer access the Internet.

The ISG50 automatically updates address objects based on an interface’s IP address, subnet, or gateway if the interface’s IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

I cannot get the RADIUS server to authenticate the ISG50‘s default admin account.

The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 48 on page 631 for more information about authentication methods.)

The ISG50 fails to authentication the ext-user user accounts I configured.

An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts. If the ISG50 tries to use the local database to authenticate an **ext-user**, the authentication attempt will always fail. (This is related to AAA servers and authentication methods, which are discussed in Chapter 48 on page 631 and Chapter 49 on page 639, respectively.)

I cannot add the admin users to a user group with access users.

You cannot put access users and admin users in the same user group.

I cannot add the default admin account to a user group.

You cannot put the default **admin** account into any user group.

The schedule I configured is not being applied at the configured times.

Make sure the ISG50’s current date and time are correct.

I cannot get a certificate to import into the ISG50.

1 For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the ISG50. You can also import a certificate in PKCS#12 format, including the certificate’s public and private keys.

2 You must remove any spaces from the certificate’s filename before you can import the certificate.

3 Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The ISG50 currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ISG50.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

I cannot access the ISG50 from a computer connected to the Internet.

Check the service control rules and to-ISG50 firewall rules.

I uploaded a logo to display on the upper left corner of the Web Configurator login screen and access page but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

I uploaded a logo to use as the screen or window background but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

The ISG50's traffic throughput rate decreased after I started collecting traffic statistics.

Data collection may decrease the ISG50's traffic throughput rate.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ISG50 treat the line as a comment.
- Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ISG50 exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the ISG50 restarts. You could use multiple `write` commands in a long script.

Note: “exit” or “!'” must follow sub commands if it is to make the ISG50 exit sub command mode.

See Chapter 55 on page 725 for more on configuration files and shell scripts.

I cannot get the firmware uploaded using the commands.

The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

My packet capture captured less than I wanted or failed.

The packet capture screen’s **File Size** sets a maximum size limit for the total combined size of all the capture files on the ISG50, including any existing capture files and any new capture files you generate. If you have existing capture files you may need to set this size larger or delete existing capture files.

The ISG50 stops the capture and generates the capture file when either the capture files reach the **File Size** or the time period specified in the **Duration** field expires.

My earlier packet capture files are missing.

New capture files overwrite existing files of the same name. Change the **File Suffix** field’s setting to avoid this.

61.1 Resetting the ISG50

If you cannot access the ISG50 by any method, try restarting it by turning the power off and then on again. If you still cannot access the ISG50 by any method or you forget the administrator password(s), you can reset the ISG50 to its factory-default settings. Any configuration files or shell scripts that you saved on the ISG50 should still be available afterwards.

Use the following procedure to reset the ISG50 to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

If you want to reboot the device without changing the current configuration, see Chapter 58 on page 753.

1. Make sure the **SYS** LED is on and not blinking.
2. Press the **RESET** button and hold it until the **SYS** LED begins to blink. (This usually takes about five seconds.)
3. Release the **RESET** button, and wait for the ISG50 to restart.

You should be able to access the ISG50 using the default settings.

61.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

Log Descriptions

This appendix provides descriptions of example log messages for the ISG50. The logs do not all apply to all of the ISG50s. You will not necessarily see all of these logs in your device.

The PBX call service logs deal with call service errors.

Table 308 PBX Call Service Logs

LOG MESSAGE	DESCRIPTION
`The call from extension %s was hung up due to emergency call is coming.`	The listed extension's call was disconnected to free up resources for an emergency call. 1st %s: Extension number 2nd %s: Emergency channel name
`Direct pickup was failed due to no call was found for extension '%s'.`	Direct pickup failed because no call was found for the listed extension. 1st %s: Extension number
`The call in hunt group or ACD skill was hung up due to timeout.`	Leaving hunt group or ACD skill due to timeout.
`Set %s to system default MOH failed due to sound file was missing.`	Setting the listed Music on Hold profile as the system default failed. 1st %s: Music on Hold profile name
`Loading Customized Auto Attendant sound file package was failed due to mismatch. Please upload correct sound file package.`	Configuration file and backup audio file does not match.
`Sound file named '%s' was uploaded successfully.`	The listed audio file was uploaded successfully. 1st %s: Upload file name
`Delete all sound files for Auto Attendant.`	Delete all audio files of AA.
`Delete unused sound files of Auto Attendant.`	Delete unused audio files of AA.
`The call was rejected due to g723 codec doesn't support in conference function`	The call was rejected because the conference function doesn't support the g.723 codec.

Table 308 PBX Call Service Logs (continued)

LOG MESSAGE	DESCRIPTION
`The call was reject due to there are % memebrs in conference.`	Conference licenses have reached the maximun number of %d. 1st %s: Conference license number
`The call was reject due to teher are % memebrs in conference room %s`	The call was rejected because there are % memebrs in conference room %s . 1st %d: Count of members 2nd %s: Conference room number

The PBX supplemental service logs deal with supplemental service errors.

Table 309 PBX Supplemental Service Logs

LOG MESSAGE	DESCRIPTION
`The call can't be recorded due to usb storage is not ready.`	The call cannot be recorded because the usb storage is not ready.
`The call can't be recorded due to total recording time has reached the Call Recording Quota.`	The call cannot be recorded because the total call recording time has reached the Call Recording Quota.
`The call can't be recorded due to reach the maximum call recording license: %d.`	The call cannot be recorded because the maximum call recording license %d has been reached. 1st %s: Recoding license
`The call can't be recorded due to g.723 codec doesn't support in recording function.`	The call cannot be recorded because it is using the g.723 codec which the call recording function does not support.
`The call can not be parked due to no more parking space.`	The call cannot be parked because all of the call parking slots are full.
`The call was dropped due to codec is not compatible.`	The call was dropped because the codec is not compatible.
`There is no any DTMF can be detected while call transfer.`	The ISG50 did not detect any DTMF during the call transfer.
`The call that parked by extension %s was timeout.`	The call parked by extension %s timed out. 1st %s: Extension name
`Group pickup was failed due to no incoming call was found.`	Group pickup did not work because there was no available call to pick up.
`Call transfer timeout. Extension: %s Collected digit: '%s.`	An attempted call transfer timed out before enough digits were detected to complete the transfer. [%s Collected: '%s'] 1st %s: Extension Number 2nd %d: Collected digit

The PBX dialplan logs deal with dialplan information and errors..

Table 310 PBX Dialplan Logs

LOG MESSAGE	DESCRIPTION
`ACD agent %s called to extension %s has failed due to extension is busy.`	The call failed because the ACD agent was busy. 1st %s: Agent number 2nd %s: Extension Number
`ACD agent %s call to extension %s has failed due to extension didn't answer.`	The call failed because the ACD agent did not answer. 1st %s: Agent number 2nd %s: Extension Number
`ACD agent %s call to extension %s has failed due to extension didn't register.`	The call failed because the ACD agent was not registered. 1st %s: Agent number 2nd %s: Extension Number
`ACD agent %s call to extension %s has failed due to extension rejected the call.`	The call failed because the ACD agent rejected the call. 1st %s: Agent number 2nd %s: Extension Number
`Auto Callback booking calls have reached the maximum number of %s.`	Auto callback booking calls have reached the maximum number.
`Dial emergency call %s%s through outbound line %s failed due to outbound line is %s.`	Dialing an emergency call failed the first time. 1st %s: Emergency call prefix 2nd %s: Emergency number 3rd %s: Outbound line name 4th %s: Dial status (busy...)
`Emergency call second retry failed. Dial emergency call %s%s through outbound line %s failed due to outbound line is %s.`	Dialing an emergency call failed a second time. 1st %s: Emergency call prefix 2nd %s: Emergency number 3rd %s: Outbound line name 4th %s: Dial status (busy...)
`Emergency call third retry failed. Dial emergency call %s%s through outbound line %s failed due to outbound line is %s.`	Dialing an emergency call failed a third time. 1st %s: Emergency call prefix 2nd %s: Emergency number 3rd %s: Outbound line name 4th %s: Dial status (busy...)
`The call forwarded to %s failed due to forward to caller number.`	A call failed because the ISG50 could not forward it to the caller number.
`The call forwarded to extension %s failed due to the call was not answered.`	A forwarded call failed because it was not answered. 1st %s: Forward number

Table 310 PBX Dialplan Logs (continued)

LOG MESSAGE	DESCRIPTION
`The call from extension %s was blocked due to no caller ID.`	A call from the specified extenstion was blocked because it did not provide caller ID.
`The call from extension was blocked due to caller id is in callee block list.`	A call was blocked because the caller ID is in the callee's block list. 1st %s: Caller ID 2nd %s: Callee number
`The call from extension %s to extension %s has been forwarded to voicemail due to after office hour.`	A call was forwarded to voicemail because it was not during office hours. 1st %s: Caller number 2nd %s: Callee number
`The call from extension %s was blocked due to caller id isn't in DND white list of extension %s.`	A call from the first specified extension was blocked because the caller ID is not in the callee's DND white list. 1st %s: Caller number 2nd %s: Callee number
`The call from extension %s to extension %s has been forwarded to voicemail due to DND forward.`	A call from the first specified extension to the second specified extension was forwarded to voicemail because the callee had DND set to forward to voicemail. 1st %s: Caller number 2nd %s: Callee number
`The call from extension %s to extension %s has been forwarded to voicemail due to blind foward.`	A call from the first specified extension to the second specified extension was forwarded to voicemail because the callee had blind forwarding configured. 1st %s: Caller number 2nd %s: Callee number
`Call to unregistered exntension number %s.`	A caller called to an unregistered SIP number. 1st %s: Extension number
`Call to un-plugged BRI number %s.`	A caller called to a BRI number that was not connected. 1st %s: Extension number
`The call from extension %s to extension %s has been forwarded to voicemail due no answer forward.`	A call from the first specified extension to the second specified extension was forwarded to voicemail because the callee did not answer and had no-answer forwarding configured. 1st %s: Caller number 2nd %s: peer number
`The call from extension %s to extension %s has been forwarded to voicemail due busy forward.`	A call from the first extension to the second extension was forwarded to voicemail because the callee's extension was busy. 1st %s: Caller number 2nd %s: Called number
`The incoming call presses a wrong Group Access Code.`	A caller entered an incorrect CAC code in the Auto-Attendant menu.
`The incoming call dials number %s is an invalid number.`	The incoming caller dialed an invalid number {DialNumber}. 1st %s: Caller dialed number (outgoing call)

Table 310 PBX Dialplan Logs (continued)

LOG MESSAGE	DESCRIPTION
`The incoming call dials number is an invalid number`	The incoming call dialed an invalid number.
`The incoming call does not presses any number.`	The caller did not dial any number in the Auto-Attendant menu before the time out period.
`The find-me list forward failed. There is no number configuration for find-me list on extension %s.`	Call forwarding failed because the extension did not have any numbers configured in the find-me list. 1st %s: Called number
`LCR %s accepts the dialing number %s from %s.`	The listd LCR accepted the specified dialed number from the listed caller. 1st %s: LCR name 2nd %s: Dialing number 3rd %s: Caller number
`The extension %s dials %s failed. The channel %s in LCR %s is %s.`	The listed caller failed to call the listed number via the listed trunk and LCR. 1st %s: Caller number 2nd %s: Dialing number 3rd %s: Trunk name 4th %s: LCR name 5th %s: Dial status
`The extension %s dials %s failed. The channel %s line %s in LCR %s is %s.`	The listed caller failed to call the listed number via the listed trunk, LCR, and port. 1st %s: Caller number 2nd %s: Dialing number 3rd %s: Trunk Name 4th %s: Which physical port 5th %s: LCR name 6th %s: Dial status
`Mobile extension %s logon successfully.`	The listed mobile extension logged on sucessfully. 1st %s: Mobile extension number
`Mobile extension %s logon failed. The mobile extension is an invalid number.`	The listed mobile extension failed to log on because there is no such number. 1st %s: Mobile extension number
`Mobile extension %s logon failed. The configuration is incomplete.`	The listed mobile extension failed to log on because the configuration is incomplete. 1st %s: Mobile extension number

Table 310 PBX Dialplan Logs (continued)

LOG MESSAGE	DESCRIPTION
`Mobile extension %s logon failed. The inputing PIN code is incorrect.`	The listed mobile extension failed to log on because the PIN code was not input properly. 1st %s: Mobile extension number
`Mobile extension %s logoff successfully.`	The listed mobile extension logged off sucessfully. 1st %s: Mobile extension number
`Mobile extension %s logoff failed. The mobile extension is an invalid number.`	The listed mobile extension failed to log off because there is no such number. 1st %s: Mobile extension number
`Mobile extension %s logoff failed. The configuration is incomplete.`	The listed mobile extension failed to log off because the configuration is incomplete. 1st %s: Mobile extension number
`Mobile Extension %s logoff failed. The inputing PIN code is incorrect.`	The listed mobile extension failed to log off because the PIN code was not input properly. 1st %s: Mobile extension number
`Mobile extension auto on/off feature is failed. No caller ID.`	Mobile extension auto-on-off failed. The caller does not have caller ID.
`The extension %s has an invalid mobile extension number %s.`	The mobile extension number of the extension number is invalid. 1st %s: Dialing extension number 2nd %s: Mobile extension number of dialing extension
`The extension %s change authority group from %s to %s by inputing Group Access Code.`	The specified caller input an access code to change from one authority group to another. 1st %s: Caller number 2nd %s: Original Group 3rd %s: Used CAC group
`The extension %s inputs a wrong Group Access Code %s.`	The specified caller input an incorrect access code. 1st %s: Caller number 2nd %s: Input CAC code

The PBX SIP logs deal with SIP information and errors.

Table 311 PBX SIP Logs

LOG MESSAGE	DESCRIPTION
`The call %s peer '%s' was rejected due to the call reaches the call limit of %d.`	The call was rejected becaure it exceeded the call limit. 1st %s: Call direction, from or to 2nd%s: Peer name, 3rd%d: Call limit
`The call was rejected by peer device %s. Received 403 Forbidden SIP reply from peer device.`	The call was rejected by the peer device. 1st %s: Peer device (403 Forbidden SIP reply received)
`Register failed due to wrong password on authentication. Username: %s. Server Name: %s.`	Registration failed because the wrong password was provided during authentication. (403 Forbidden SIP reply received) 1st %s: Username 2nd %s: Hostname
`The call was rejected due to autentication failed for peer device %s.`	The call was rejected because authentication failed for the peer device. 1st %s: Peer device
`The call to extension %s was rejected due to extension %s not found.`	The call was rejected because the extension could not be found. (Recieved “404 not found” SIP packet)
`Call from %s to extension %s was rejected due to extension not found. Context: %s.`	The call was rejected because the called number was not found in the context. 1st %s: Username/peername 2nd %s: Extension 3rd %s: Context
`Address is wrong while register to %s@%s, giving up (check config).`	The ISG50 received a 479 error because it was not able to process the URI SIP reply and is giving up its attemps to register the listed user name and hostname. 1st %s: Username 2nd %s: Hostname
`The call to device %s is rejected due to too many calls.`	A call to the listed device failed because there are too many calls. %s: Username
`The call to device %s is rejected due to too many calls.`	Failed to start the PBX because the call limit has been reached. 1st %s: Username
`Call failed due to network loop detected.`	A call failed because a network loop was detected.
`Call from '%s' to extension '%s' was rejected due to callee address incomplete.`	The call was rejecteddbecause the callee’s address was incomplete. 1st %s: Caller number 2nd %s: Called number

Table 311 PBX SIP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Call rejected due to SDP issue (Got "488 Not acceptable here").`	There was an SDP processing error.
`Call rejected due to unacceptable codecs..`	The call was rejected because of unacceptable codecs (received a 488 Not acceptable here SIP reply).
`Call rejected due to callee does not support required crypto.`	The target does not support required encryption.
`Call rejected due to no compatible codecs.`	The call was rejected due to a codec error.
`The call to device %s is rejected due to PBX service unavailable.`	The call was rejected because the PBX service was unavailable. 1st %s: Called number
`Call rejected due to no one pick up call for %s in pick up group.`	No one picked up the listed call. 1st %s: Call ID
`Call rejected due to can not find call (no channel).`	Unable to create or find the SIP channel for this INVITE.
`The call %s peer '%s' was rejected due to the call reaches the call limit of %d.`	The call was rejected because it exceeded the call limit. 1st %s: Call direction, "from" or "to" 2nd %s: Peer name %d: Call limit
`The call is failed due to no compatible codecs.`	The call was not accepted because there were no compatible codecs.
`Extension '%s' was unregistered due to time expired.`	The SIP peer was deregistered because its time expired. 1st %s: Peer name
`Extension '%s' requested to unregister.`	The SIP peer deregistered. 1st %s: Peer name
`The expire time is set as %d due to extension %s is behind NAT.`	The device is behind NAT and its expire time is {Expire_time}. 1st %d: Expire time
`Extension '%s' registered successfully at %s with expire time %d.`	Peer registered successfully with the expire time {Expire_time}. 1st %s: Peer name 2nd %s: IP or hostname 1st %d: Expire time
`SIP trunk registered successfully to '%s@%s'.`	The SIP trunk registered successfully to the listed user name and host name. 1st %s: User name 2nd %s: Host name

Table 311 PBX SIP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Unknown SIP response. Response code: %d. Response method: %s. Address: %s.`	The ISG50 received an unknown SIP response. 1st %d: Response code 1st %s: Response method 2nd %s: Address
`Registration from extension '%s' failed for '%s'. Reason: %s.`	The listed extension's registration failed. 1st %s: "To" header from Request 2nd %s: Request address 3rd %s: Reason
`The call can't be configured as peer-to-peer call. Reason: Peer should be behind NAT.`	The call could not be made as a peer to peer call because at least 1 phone is behind NAT.
`The call can't be configured as peer-to-peer call. Reason: PBX should behind NAT, and peer should be in local net.`	There was a peer to peer exception. The PBX should be behind NAT and peers should be on the local network.
`The call can't be configured as peer-to-peer call. Reason: At least one peer is at different WAN/LAN.`	This is due to a peer to peer exception; at least 1 phone is at a different WAN/LAN.
`The call can't be configured as peer-to-peer call. Reason: Peer-to-peer local net hasn't been set up.`	This is due to a peer to peer exception. The peer to peer local net is not set up.
`The call can't be configured as peer-to-peer call. Reason: At least one peer DTMF is not INFO.`	This is due to a peer to peer exception. At least 1 phone's DTMF is not set to INFO.
`The call can't be configured as peer-to-peer call. Reason: Codec is different.`	This peer to peer exception is due to different codecs.
`The call can't be configured as peer-to-peer call. Reason: Call recording is enabled.`	This peer to peer exception is due to at least 1 peer enabling call recording .
`No more available RTP port. Please enlarge the RTP port range`	No more available RTP ports. Please enlarge the RTP port range.

The PBX trunk logs deal with the SIP trunk being disconnected or recovered.

Table 312 PBX Trunk Logs

LOG MESSAGE	DESCRIPTION
`The SIP trunk %s is disconnected.`	The SIP trunk %s is disconnected. 1st %s: SIP Trunk name
`The SIP trunk %s is disconnected over %d minutes.`	The SIP trunk %s has been disconnected for over %d mins. 1st %s: SIP Trunk name
`The SIP trunk %s is recovered.`	The SIP trunk %s is recovered. 1st %s: SIP Trunk name

The PBX DSP logs deal with the Digital Signal Processor.

Table 313 PBX DSP Logs

LOG MESSAGE	DESCRIPTION
`DSP initialization has failed.`	DSP initialization has failed.
`DSP initialization has succeeded.`	DSP initialization has succeeded.

The PBX physical port logs deal with the ISG50's physical PBX ports.

Table 314 PBX Physical Port Logs

LOG MESSAGE	DESCRIPTION
`BRI port %u initialization has succeeded.`	Initialization of the listed BRI port succeeded. 1st %u:port number
`BRI port %u initialization has failed.`	Initialization of the listed BRI port failed. 1st %u: Port number
`BRI port %u is up.`	The listed BRI port is online. 1st %u: Port number
`BRI port %u is down.`	The listed BRI port is offline. 1st %u: Port number
`FXO initialization has succeeded.`	FXO module initialization succeeded.
`FXO initialization has failed.`	FXO module initialization failed.
`FXO port %u is up.`	The listed FXO port is online. 1st %u: Port number

Table 314 PBX Physical Port Logs (continued)

LOG MESSAGE	DESCRIPTION
`FXO port %u is down.`	The listed FXO port is offline. 1st %u: Port number
`FXS initialization has succeeded.`	FXS module initialization succeeded.
`FXS initialization has failed.`	FXS module initialization failed.

Table 315 PBX Default Logs

LOG MESSAGE	DESCRIPTION
`Extension '%s' makes call to extension '%s' is terminated due to the Max. Call Time timeout.`	The call from the caller ${CallerNumber} to the called ${CalledNumber} was terminated due to exceeding the Maximum Call Time timeout. 1st %s: Caller number 2nd %s: Called number
`System internal error. Failed to load PBX module %s - %s.`	Failed to load the specified PBX module. 1st %s: Module name 2nd %s: required/not required
`System internal error. Unable to open PBX modules directory '%s'.`	Unable to open the specified directory $(Path}, which the PBX modules require. 1st %s: Directory name
`Attendant console license is not enough. Total license: %d.`	The number of attendant console licenses is not enough: license ${LicenseNumber} 1st %s: License number
`Softphone license is not enough. Total license: %d.`	The number of Webphone licenses is not enough. license ${LicenseNumber} 1st %s: License number
`Extension license is not enough. Total license: %d.`	The number of extension licenses is not enough. license ${LicenseNumber} 1st %s: License number
`Local phonebook importing failed. Row number [%d] format error.`	The listed phonebook row has a format error. 1st %d: The Xth row
`Local phonebook items had reached maximum.`	The maximum number of local phonebook items has been reached.
`Import Local phonebook successfully with %d items.`	The specified number of local phonebook rows were imported successfully. %d: Phonebook row count
`Phonebook LDAP search timeout.`	The LDAP search timed out while running an automatic LDAP phonebook update.
`Phonebook LDAP server address is empty.`	The ISG50 tried to perform an automatic LDAP phonebook update and found that the LDAP server address was not configured.

Table 315 PBX Default Logs (continued)

LOG MESSAGE	DESCRIPTION
`Phonebook LDAP server Base DN is empty.`	The ISG50 tried to perform an automatic LDAP phonebook update and found that the LDAP server Base DN was not configured.
`LDAP phonebook refresh failed due to LDAP is not activate.`	The LDAP phonebook refresh failed because the LDAP server was not active.
`Phonebook LDAP server update failed due to wrong server IP or port.`	The phonebook LDAP server update failed because the wrong server IP or port was configured.
`Phonebook LDAP server update failed due to wrong bind DN or password`	The phonebook LDAP server update failed because the wrong bind DN or password was configured.
`Phonebook LDAP server update failed.`	An automatic LDAP phonebook update failed.
`File convert from %s to %s was failed`	Converting a file from ${SrcFile} to ${DstFile} failed. 1st %s: Source file 2nd %s: Destination file
`Extension %s request rejected due to the extension has been locked`	A request for the specified extension ${ExtensionNumber} was rejected due to the extension being locked. 1st %s: Extension number
`Extension %s request failed due to incorrect password. Fail count: %d`	A request for the specified extension ${ExtensionNumber} failed due to an incorrect password. Fail count ${Count} 1st %s: Extension number 2nd %s: Count
`Extension %s has been locked due to request retry fail reach %d times`	Extension ${ExtensionNumber} has been locked because the request retry fail count reached a certain number ${Count} of times. 1st %s: Extension number 2nd %s: Count
`Extension %s login rejected due to the extension has been locked`	The extension login was rejected due to the extension being locked. 1st %s: Extension number
`Extension %s login failed due to incorrect PIN code. Fail count: %d`	The extension login failed a consecutive number of times {Count} due to an incorrect PIN code. 1st %s: Extension number 2nd %s: Count
`Extension %s has been locked due to login retry fail reach %d times.`	The extension has been locked due to the login retry fail count reaching a certain number ${Count} of times. 1st %s: Extension number 2nd %s: Count
`Failed login attempt to Extension Portal`	There was a failed extension portal login attempt.

Table 315 PBX Default Logs (continued)

LOG MESSAGE	DESCRIPTION
`Failed login attempt to Extension Portal due to the extesion is blank`	An extension portal login attempt failed due to the extesion being blank.
`Extension [%s] has logged in Extension Portal`	The user of the specified extension {Extension Number} has logged into the extension portal. 1st %s: Extension number

The ZySH logs deal with internal system errors.

Table 316 ZySH Logs

LOG MESSAGE	DESCRIPTION
`Invalid message queue. Maybe someone starts another zysh daemon.`	
`ZySH daemon is instructed to reset by %d`	1st:pid num
`System integrity error!`	
`Group OPS`	
`cannot close property group`	
`cannot close group`	
`%s: cannot get size of group`	1st:zysh group name
`%s: cannot specify properties for entry %s`	1st:zysh group name, 2st:zysh entry name
`%s: cannot join group %s, loop detected`	1st:zysh group name, 2st:zysh group name
`cannot create, too many groups (>%d)`	1st:max group num
`%s: cannot find entry %s`	1st:zysh group name, 2st:zysh entry name
`%s: cannot remove entry %s`	1st:zysh group name, 2st:zysh entry name
`List OPS`	
`can't alloc entry: %s!`	1st:zysh entry name
`can't retrieve entry: %s!`	1st:zysh entry name
`can't get entry: %s!`	1st:zysh entry name
`can't print entry: %s!`	1st:zysh entry name
`%s: cannot retrieve entries from list!`	1st:zysh list name
`can't get name for entry %d!`	1st:zysh entry index

Table 316 ZySH Logs (continued)

LOG MESSAGE	DESCRIPTION
`can't get reference count: %s!`	1st:zysh list name
`can't print entry name: %s!`	1st:zysh entry name
`Can't append entry: %s!`	1st:zysh entry name
`Can't set entry: %s!`	1st:zysh entry name
`Can't define entry: %s!`	1st:zysh entry name
`%s: list is full!`	1st:zysh list name
`Can't undefine %s`	1st:zysh list name
`Can't remove %s`	1st:zysh list name
Table OPS	
`%s: cannot retrieve entries from table!`	1st:zysh table name
`%s: index is out of range!`	1st:zysh table name
`%s: cannot set entry #%d`	1st:zysh table name,2st: zysh entry num
`%s: table is full!`	1st:zysh table name
`%s: invalid old/new index!`	1st:zysh table name
`Unable to move entry #%d!`	1st:zysh entry num
`%s: invalid index!`	1st:zysh table name
`Unable to delete entry #%d!`	1st:zysh entry num
`Unable to change entry #%d!`	1st:zysh entry num
`%s: cannot retrieve entries from table!`	1st:zysh table name
`%s: invalid old/new index!`	1st:zysh table name
`Unable to move entry #%d!`	1st:zysh entry num
`%s: apply failed at initial stage!`	1st:zysh table name
`%s: apply failed at main stage!`	1st:zysh table name
`%s: apply failed at closing stage!`	1st:zysh table name

Table 317 ADP Logs

LOG MESSAGE	DESCRIPTION
`from <zone> to <zone> [type=<type>] <message> , Action: <action>, Severity: <severity>`	The ISG50 detected an anomaly in traffic traveling between the specified zones. The <type> = {scan-detection(<attack>) | flood-detection(<attack>) | http-inspection(<attack>) | tcp-decoder(<attack>)}. The <message> gives details about the attack, although the message is dropped if the log is more than 128 characters. The <action> is what the ISG50 did with the packet. The <severity> is the threat level (very low, low, medium, high, or severe).
`Enable ADP succeeded.`	ADP was turned on.
`Disable ADP succeeded.`	ADP was turned off.
`ADP rule <num> has been deleted.`	The specified ADP rule has been deleted.
`ADP rule <num> has been moved to <num>.`	The ADP rule with the specified index number (first num) was moved to the specified index number (second num).
`New ADP rule has been appended.`	An ADP rule has been added to the end of the list.
`ADP rule <num> has been inserted.`	An ADP rule has been inserted. <num> is the number of the new rule.
`ADP rule <num> has been modified.`	The ADP rule of the specified number has been changed.
`ADP profile <name> has been deleted.`	The ADP rule with the specified name has been removed.
`ADP profile <name> has been changed to <name>.`	An ADP rule's name has been changed from first <name> to the second <name>.
`ADP profile <name> has been created.`	An ADP profile with the specified name has been added.
`ADP profile <name> has been modified.`	The ADP rule with the specified name has been changed.
`Packet payload length is over the maximum system handle length`	The ISG50's ADP feature detected a packet with a length over 16000 bytes.
`LAND attack packet. Source IP is the same as Destination IP.`	The ISG50's ADP feature detected traffic with the same IP address set as both the source and the destination.

Table 318 User Logs

LOG MESSAGE	DESCRIPTION
`%s %s from %s has logged in ISG50`	A user logged into the ISG50. 1st %s: The type of user account. 2nd %s: The user's user name. 3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console).
`%s %s from %s has logged out ISG50`	A user logged out of the ISG50. 1st %s: The type of user account. 2nd %s: The user's user name. 3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console).
`%s %s from %s has been logged out ISG50 (re-auth timeout)`	The ISG50 is signing the specified user out due to a re-authentication timeout. 1st %s: The type of user account. 2nd %s: The user's user name. 3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console).
`%s %s from %s has been logged out ISG50 (lease timeout)`	The ISG50 is signing the specified user out due to a lease timeout. 1st %s: The type of user account. 2nd %s: The user's user name. 3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console).
`%s %s from %s has been logged out ISG50 (idle timeout)`	The ISG50 is signing the specified user out due to an idle timeout. 1st %s: The type of user account. 2nd %s: The user's user name. 3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console).
`Console has been put into lockout state`	Too many failed login attempts were made on the console port so the ISG50 is blocking login attempts on the console port.
`Address %u.%u.%u.%u has been put into lockout state`	Too many failed login attempts were made from an IP address so the ISG50 is blocking login attempts from that IP address. %u.%u.%u.%u: the source address of the user's login attempt
`Failed login attempt to ISG50 from %s (login on a lockout address)`	A login attempt came from an IP address that the ISG50 has locked out. %u.%u.%u.%u: the source address of the user's login attempt
`Failed login attempt to ISG50 from %s (reach the max. number of user)`	The ISG50 blocked a login because the maximum login capacity for the particular service has already been reached. %s: service name

Table 318 User Logs (continued)

LOG MESSAGE	DESCRIPTION
`Failed login attempt to ISG50 from %s (reach the max. number of simultaneous logon)`	The ISG50 blocked a login because the maximum simultaneous login capacity for the administrator or access account has already been reached. %s: service name
`User %s has been denied access from %s`	The ISG50 blocked a login according to the access control configuration. %s: service name
`User %s has been denied access from %s`	The ISG50 blocked a login attempt by the specified user name because of an invalid user name or password. 2nd %s: service name

Table 319 myZyXEL.com Logs

LOG MESSAGE	DESCRIPTION
`Send registration message to MyZyXEL.com server has failed.`	The device was not able to send a registration message to MyZyXEL.com.
`Get server response has failed.`	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
`Timeout for get server response.`	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
`User has existed.`	The user name already exists in MyZyXEL.com's database. So the user can't use it for device registration and needs to specify another one.
`User does not exist.`	The user name does not yet exist in MyZyXEL.com's database. So the user can use it for device registration.
`Internal server error.`	MyZyXEL.com's database had an error when checking the user name.
`Device registration has failed:%s.`	Device registration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by the myZyXEL.com server
`Device registration has succeeded.`	The device registered successfully with the myZyXEL.com server.
`Registration has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`%s:Trial service activation has failed:%s.`	Trail service activation failed for the specified service, an error message returned by the MyZyXEL.com server will be appended to this log. 1st %s: service name 2nd %s: error message returned by the myZyXEL.com server
`%s:Trial service activation has succeeded.`	Trail service was activated successfully for the specified service. %s: service name

Table 319 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Trial service activation has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`Standard service activation has failed:%s.`	Standard service activation failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by the myZyXEL.com server
`Standard service activation has succeeded.`	Standard service activation has succeeded.
`Standard service activation has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`Service expiration check has failed:%s.`	The service expiration day check failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by myZyXEL.com server
`Service expiration check has succeeded.`	The service expiration day check was successful.
`Service expiration check has failed. Because of lack must fields.`	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
`Server setting error.`	The device could not retrieve the myZyXEL.com server's IP address or FQDN from local.
`Resolve server IP has failed.`	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
`Verify server's certificate has failed.`	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate.
`Connect to MyZyXEL.com server has failed.`	The device could not connect to the MyZyXEL.com server.
`Do account check.`	The device started to check whether or not the user name in MyZyXEL.com's database.
`Do device register.`	The device started device registration.
`Do trial service activation.`	The device started trail service activation.
`Do standard service activation.`	The device started standard service activation.
`Do expiration check.`	The device started the service expiration day check.
`Build query message has failed.`	Some information was missing in the packets that the device sent to the MyZyXEL.com server.
`Parse receive message has failed.`	The device cannot parse the response returned by the MyZyXEL.com server. Maybe some required fields are missing.
`Resolve server IP has failed. Update stop.`	The update has stopped because the device couldn't resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().

Table 319 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Verify server's certificate has failed. Update stop.`	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate. The update has stopped.
`Send download request to update server has failed.`	The device's attempt to send a download message to the update server failed.
`Get server response has failed.`	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
`Timeout for get server response.`	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
`Send update request to update server has failed.`	The device could not send an update message to the update server.
`Update has failed. Because of lack must fields.`	The device received an incomplete response from the update server and it caused a parsing error for the device.
`Update server is busy now. File download after %d seconds.`	The update server was busy so the device will wait for the specified number of seconds and send the download request to the update server again.
`Device has latest file. No need to update.`	The device already has the latest version of the file so no update is needed.
`Device has latest signature file; no need to update`	The device already has the latest version of the signature file so no update is needed.
`Connect to update server has failed.`	The device cannot connect to the update server.
`Wrong format for packets received.`	The device cannot parse the response returned by the server. Maybe some required fields are missing.
`Server setting error. Update stop.`	The device could not resolve the update server's FQDN to an IP address through gethostbyname(). The update process stopped.
`Build query message failed.`	Some information was missing in the packets that the device sent to the server.
`Resolve server IP has failed.`	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
`Connect to MyZyXEL.com server has failed.`	The device could not connect to the MyZyXEL.com server.
`Build query message has failed.`	Some information was missing in the packets that the device sent to the server.
`Verify server's certificate has failed.`	The device could not process an HTTPS connection because it could not verify the server's certificate.
`Get server response has failed.`	The device sent packets to the server, but did not receive a response. The root cause may be that the connection is abnormal.

Table 319 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Expiration daily-check has failed:%s.`	The daily check for service expiration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by myZyXEL.com server
`Do expiration daily-check has failed. Because of lack must fields.`	The device received an incomplete response to the daily service expiration check and the packets caused a parsing error for the device.
`Server setting error.`	The device could not retrieve the server's IP address or FQDN from local.
`Do expiration daily-check has failed.`	The daily check for service expiration failed.
`Do expiration daily-check has succeeded.`	The daily check for service expiration was successful.
`Expiration daily-check will trigger PPP interface. Do self-check.`	Before the device sends an expiration day check packet, it needs to check whether or not it will trigger a PPP connection.
`System bootup. Do expiration daily-check.`	The device processes a service expiration day check immediately after it starts up.
`After register. Do expiration daily-check immediately.`	The device processes a service expiration day check immediately after device registration.
`Time is up. Do expiration daily-check.`	The processes a service expiration day check every 24 hrs.
`Read MyZyXEL.com storage has failed.`	Read data from EEPROM has failed.
`Open /proc/MRD has failed.`	This error message is shown when getting MAC address.
`Unknown TLS/SSL version: %d.`	The device only supports SSLv3 protocol. %d: SSL version assigned by client.
`Load trusted root certificates has failed.`	The device needs to load the trusted root certificate before the device can verify a server's certificate. This log displays if the device failed to load it.
`Certificate has expired.`	Verification of a server’s certificate failed because it has expired.
`Self signed certificate.`	Verification of a server’s certificate failed because it is self-signed.
`Self signed certificate in certificate chain.`	Verification of a server’s certificate failed because there is a self-signed certificate in the server’s certificate chain.
`Verify peer certificates has succeeded.`	The device verified a server’s certificate while processing an HTTPS connection.

Table 319 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Certification verification failed: Depth: %d, Error Number(%d):%s.`	Verification of a server's certificate failed while processing an HTTPS connection. This log identifies the reason for the failure. 1st %d: certificate chain level 2nd %d: error number %s: error message
`Certificate issuer name:%s.`	Verification of the specified certificate failed because the device could not get the certificate's issuer name. %s is the certificate name.
`The wrong format for HTTP header.`	The header format of a packet returned by a server is wrong.
`Timeout for get server response.`	After the device sent packets to a server, the device did not receive any response from the server. The root cause may be a network delay issue.
`Download file size is wrong.`	The file size downloaded for AS is not identical with content-length
`Parse HTTP header has failed.`	Device can't parse the HTTP header in a response returned by a server. Maybe some HTTP headers are missing.

Table 320 IKE Logs

LOG MESSAGE	DESCRIPTION
`Peer has not announced DPD capability`	The remote IPSec router has not announced its dead peer detection (DPD) capability to this device.
`[COOKIE] Invalid cookie, no sa found`	Cannot find SA according to the cookie.
`[DPD] No response from peer. Using existing Phase-1 SA in %u seconds. Trying with Phase-1 rekey.`	The device's DPD feature has not detected a response from the remote IPSec router. %u is the retry time.
`[HASH] : Tunnel [%s] Phase 1 hash mismatch`	%s is the tunnel name. When negotiating Phase-1, the exchange hash did not match.
`[HASH] : Tunnel [%s] Phase 2 hash mismatch"`	%s is the tunnel name. When negotiating Phase-2, the calculated quick mode authentication hash did not match.
`[ID] : Invalid ID information`	ID payload is not valid (in Phase-1 is local/peer ID, in Phase-2 is local/remote policy).
`[ID] : Tunnel [%s] Local IP mismatch`	%s is the tunnel name. When negotiating Phase-1, the local tunnel IP did not match the My IP in VPN gateway.
`[ID] : Tunnel [%s] My IP mismatch`	%s is the tunnel name. When negotiating Phase-1 and selecting matched proposal, My IP Address could not be resolved.
`[ID] : Tunnel [%s] Phase 1 ID mismatch`	%s is the tunnel name. When negotiating Phase-1, the peer ID did not match.
`[ID] : Tunnel [%s] Phase 2 Local ID mismatch`	%s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.

Table 320 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`[ID] : Tunnel [%s] Phase 2 Remote ID mismatch`	%s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.
`[ID] : Tunnel [%s] Remote IP mismatch`	%s is the tunnel name. When negotiating Phase-1, the peer tunnel IP did not match the secure gateway address in VPN gateway.
`[SA] : Malformed IPSec SA proposal`	When selecting a matched proposal, some protocol was given more than once.
`[SA] : No proposal chosen`	When selecting a matched proposal in phase-1 or phase-2, so proposal was selected.
`[SA] : Tunnel [%s] Phase 1 authentication algorithm mismatch`	%s is the tunnel name. When negotiating Phase-1, the authentication algorithm did not match.
`[SA] : Tunnel [%s] Phase 1 authentication method mismatch`	%s is the tunnel name. When negotiating Phase-1, the authentication method did not match.
`[SA] : Tunnel [%s] Phase 1 encryption algorithm mismatch`	%s is the tunnel name. When negotiating Phase-1, the encryption algorithm did not match.
`[SA] : Tunnel [%s] Phase 1 invalid protocol`	%s is the tunnel name. When negotiating Phase-1, the packet was not a ISKAMP packet in the protocol field.
`[SA] : Tunnel [%s] Phase 1 invalid transform`	%s is the tunnel name. When negotiating Phase-1, the transform ID was invalid.
`[SA] : Tunnel [%s] Phase 1 key group mismatch`	%s is the tunnel name. When negotiating Phase-1, the DH group of the attribute list `attrs' did not match the security policy.
`[SA] : Tunnel [%s] Phase 1 negotiation mode mismatch`	%s is the tunnel name. When negotiating Phase-1, the negotiation mode did not match.
`[SA] : Tunnel [%s] Phase 2 authentication algorithm mismatch`	%s is the tunnel name. When negotiating Phase-2, the authentication algorithm did not match.
`[SA] : Tunnel [%s] Phase 2 encapsulation mismatch`	%s is the tunnel name. When negotiating Phase-2, the encapsulation did not match.
`[SA] : Tunnel [%s] Phase 2 encryption algorithm mismatch`	%s is the tunnel name. When negotiating Phase-2, the encryption algorithm did not match.
`[SA] : Tunnel [%s] Phase 2 pfs mismatch`	%s is the tunnel name. When negotiating Phase-2, the PFS specified did not match.
`[SA] : Tunnel [%s] Phase 2 pfs unsupported: %d`	%s is the tunnel name. When negotiating Phase-2, this device does not support the PFS specified.
`[SA] : Tunnel [%s] Phase 2 SA encapsulation mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA encapsulation did not match.

Table 320 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`[SA] : Tunnel [%s] Phase 2 SA protocol mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA protocol did not match.
`[SA] : Tunnel [%s] SA sequence size mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA sequence size did not match.
`[XCHG] exchange type is not IP, AGGR, or INFO`	This device is the responder and this is the initiator’s first packet, but exchange type is not IP, AGGR, or INFO and the packet is ignored.
`Cannot resolve My IP Addr %s for Tunnel [%s]`	1st %s is my ip address. 2nd %s is the tunnel name. When selecting a matched proposal in phase-1, the engine could not get My-IP address.
`Cannot resolve Secure Gateway Addr %s for Tunnel [%s]`	1st %s is my ip address. 2nd %s is the tunnel name; When selecting a matched proposal in phase-1, the engine could not get the correct secure gateway address.
`Could not dial dynamic tunnel "%s"`	%s is the tunnel name. The tunnel is a dynamic tunnel and the device cannot dial it.
`Could not dial incomplete tunnel "%s"`	%s is the tunnel name. The tunnel setting is not complete.
`Could not dial manual key tunnel "%s"`	%s is the tunnel name. The manual key tunnel cannot be dialed.
`DPD response with invalid ID`	When receiving a DPD response with invalid ID ignored.
`DPD response with no active request`	When receiving a DPD response with no active query.
`IKE Packet Retransmit`	When retransmitting the IKE packets.
`Phase 1 IKE SA process done`	When Phase 1 negotiation is complete.
`Recv Main Mode request from [%s]`	%s is the remote name; When receiving a request to enter Main mode.
`Recv Aggressive Mode request from [%s]`	%s is the remote name; When receiving a request to enter Aggressive mode.
`Recv:[SA][KE][ID][CERT][CR][HASH][SIG][NONCE][DEL][VID][ATTR][NOTFY:%s]`	This is a combined message for incoming IKE packets
`Send Main Mode request to [%s]`	%s is the remote name. The device sent a request to enter Main Mode.
`Send Aggressive Mode request to [%s]`	%s is the remote name. The device sent a request to enter Aggressive Mode.
`Send:[SA][KE][ID][CERT][CR][HASH][SIG][NONCE][DEL][VID][ATTR][NOTFY:%s]`	This is a combined message for outgoing IKE packets.
`Start Phase 2: Quick Mode`	Indicates the beginning of phase 2 using quick mode.

Table 320 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`The cookie pair is : 0x%08x%08x / 0x%08x%08x`	Indicates the initiator/responder cookie pair.
`The IPSec tunnel "%s" is already established`	%s is the tunnel name. When dialing a tunnel, the tunnel is already dialed.
`Tunnel [%s] built successfully`	%s is the tunnel name. The phase-2 tunnel negotiation is complete.
`Tunnel [%s] Phase 1 pre-shared key mismatch`	%s is the tunnel name. When negotiating phase-1, the pre-shared key did not match.
`Tunnel [%s] Recving IKE request`	%s is the tunnel name. The device received an IKE request.
`Tunnel [%s] Sending IKE request`	%s is the tunnel name. The device sent an IKE request.
`Tunnel [%s] IKE Negotiation is in process`	%s is the tunnel name. When IKE request is already sent but still attempting to dial a tunnel.
`VPN gateway %s was disabled`	%s is the gateway name. An administrator disabled the VPN gateway.
`VPN gateway %s was enabled`	%s is the gateway name. An administrator enabled the VPN gateway.
`XAUTH fail! My name: %s`	%s is the my xauth name. This indicates that my name is invalid.
`XAUTH fail! Remote user: %s`	%s is the remote xauth name. This indicates that a remote user’s name is invalid.
`XAUTH succeed! My name: %s`	%s is the my xauth name. This indicates that my name is valid.
`XAUTH succeed! Remote user: %s`	%s is the remote xauth name. This indicate that a remote user’s name is valid
`Dynamic Tunnel [%s:%s:0x%x:%s] built successfully`	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
`Dynamic Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully`	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
`Tunnel [%s:%s:0x%x:%s] built successfully`	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
`Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully`	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
`Tunnel [%s:%s]  Phase 1 pre-shared key mismatch`	The variables represent the phase 1 name and tunnel name. When negotiating phase-1, the pre-shared keys did not match.
`Tunnel [%s:%s] Recving IKE request`	The variables represent the phase 1 name and tunnel name. The device received an IKE request.

Table 320 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Tunnel [%s:%s] Sending IKE request`	The variables represent the phase 1 name and tunnel name. The device sent an IKE request.
`Tunnel [%s:0x%x] is disconnected`	The variables represent the tunnel name and the SPI of a tunnel that was disconnected.
`Tunnel [%s] rekeyed successfully`	%s is the tunnel name. The tunnel was rekeyed successfully.

Table 321 IPSec Logs

LOG MESSAGE	DESCRIPTION
`Corrupt packet, Inbound transform operation fail`	The device received corrupt IPsec packets and could not process them.
`Encapsulated packet too big with length`	An outgoing packet needed to be transformed but was longer than 65535.
`Get inbound transform fail`	When performing inbound processing for incoming IPSEC packets and ICMPs related to them, the engine cannot obtain the transform context.
`Get outbound transform fail`	When outgoing packet need to be transformed, the engine cannot obtain the transform context.
`Inbound transform operation fail`	After encryption or hardware accelerated processing, the hardware accelerator dropped a packet (resource shortage, corrupt packet, invalid MAC, and so on).
`Outbound transform operation fail`	After encryption or hardware accelerated processing, the hardware accelerator dropped a packet (e.g., resource overflow, corrupt packet, and so on).
`Packet too big with Fragment Off`	An outgoing packet needed to be transformed, but the fragment flag was off and the packet was too big.
`SPI:0x%x SEQ:0x%x Execute transform step fail, ret=%d`	The variables represent the SPI, sequence number and the error number. When trying to perform transforming, the engine returned an error.
`SPI:0x%x SEQ:0x%x No rule found, Dropping packet`	The variables represent the SPI and the sequence number. The packet did not match the tunnel policy and was dropped.
`SPI:0x%x SEQ:0x%x Packet Anti-Replay detected`	The variables represent the SPI and the sequence number. The device received a packet again (that it had already received).
`VPN connection %s was disabled.`	%s is the VPN connection name. An administrator disabled the VPN connection.
`VPN connection %s was enabled.`	%s is the VPN connection name. An administrator enabled the VPN connection.
`Due to active connection allowed exceeded, %s was deleted.`	%s is the VPN connection name. The number of active connections exceeded the maximum allowed.

Table 322 Firewall Logs

LOG MESSAGE	DESCRIPTION
`priority:%lu, from %s to %s, service %s, %s`	1st variable is the global index of rule, 2nd is the from zone, 3rd is the to zone, 4th is the service name, 5th is ACCEPT/DROP/REJECT.
`%s:%d: in %s():`	Firewall is dead, trace to %s is which file, %d is which line, %s is which function
`Firewall has been %s.`	%s is enabled/disabled
`Firewall rule %d has been moved to %d.`	1st %d is the old global index of rule, 2nd %d is the new global index of rule
`Firewall rule %d has been deleted.`	%d is the global index of rule
`Firewall rules have been flushed.`	Firewall rules were flushed
`Firewall rule %d was %s.`	%d is the global index of rule, %s is appended/inserted/modified
`Firewall %s %s rule %d was %s.`	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule 3rd %s is appended/inserted/modified
`Firewall %s %s rule %d has been moved to %d.`	1st %s is from zone, 2nd %s is to zone, 1st %d is the old index of the rule 2nd %d is the new index of the rule
`Firewall %s %s rule %d has been deleted.`	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule
`Firewall %s %s rules have been flushed.`	1st %s is from zone, 2nd %s is to zone
`abnormal TCP flag attack detected`	Abnormal TCP flag attack detected
`invalid state detected`	Invalid state detected
`The Asymmetrical Route has been enabled.`	Asymmetrical route has been turned on.
`The Asymmetrical Route has been disabled.`	Asymmetrical Route has been turned off.

Table 323 Sessions Limit Logs

LOG MESSAGE	DESCRIPTION
`Maximum sessions per host (%d) was exceeded.`	%d is maximum sessions per host.

Table 324 Policy Route Logs

LOG MESSAGE	DESCRIPTION
`Can't open bwm_entries`	Policy routing can't activate BWM feature.
`Can't open link_down`	Policy routing can't detect link up/down status.
`Cannot get handle from UAM, user-aware PR is disabled`	User-aware policy routing is disabled due to some reason.
`mblock: allocate memory failed!`	Allocating policy routing rule fails: insufficient memory.
`pt: allocate memory failed!`	Allocating policy routing rule fails: insufficient memory.
`To send message to policy route daemon failed!`	Failed to send control message to policy routing manager.
`The policy route %d allocates memory fail!`	Allocating policy routing rule fails: insufficient memory. %d: the policy route rule number
`The policy route %d uses empty user group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty source address group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty destination address group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty service group`	Use an empty object group. %d: the policy route rule number
`Policy-route rule %d was inserted.`	Rules is inserted into system. %d: the policy route rule number
`Policy-route rule %d was appended.`	Rules is appended into system. %d: the policy route rule number
`Policy-route rule %d was modified.`	Rule is modified. %d: the policy route rule number
`Policy-route rule %d was moved to %d.`	Rule is moved. 1st %d: the original policy route rule number 2nd %d: the new policy route rule number
`Policy-route rule %d was deleted.`	Rule is deleted. %d: the policy route rule number
`Policy-route rules were flushed.`	Policy routing rules are cleared.
`BWM has been activated.`	The global setting for bandwidth management on the ISG50 has been turned on.
`BWM has been deactivated.`	The global setting for bandwidth management on the ISG50 has been turned off.

Table 324 Policy Route Logs (continued)

LOG MESSAGE	DESCRIPTION
`Interface %s alive, related policy route rules will be re-enabled`	An interface came back up so the ISG50 will use the related policy route rules again.
`Interface %s dead, related policy route rules will be disabled`	An interface went down so the ISG50 will stop using the related policy route rules.
`Trunk %s alive, related policy route rules will be re-enabled`	A trunk came back up so the ISG50 will use the related policy route rules again.
`Trunk %s dead, related policy route rules will be disabled`	A trunk went down so the ISG50 will stop using the related policy route rules.

Table 325 Built-in Services Logs

LOG MESSAGE	DESCRIPTION
`User on %u.%u.%u.%u has been denied access from %s`	HTTP/HTTPS/TELNET/SSH/FTP/SNMP access to the device was denied. %u.%u.%u.%u is IP address %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET
`HTTPS certificate:%s does not exist. HTTPS service will not work.`	An administrator assigned a nonexistent certificate to HTTPS. %s is certificate name assigned by user
`HTTPS port has been changed to port %s.`	An administrator changed the port number for HTTPS. %s is port number
`HTTPS port has been changed to default port.`	An administrator changed the port number for HTTPS back to the default (443).
`HTTP port has changed to port %s.`	An administrator changed the port number for HTTP. %s is port number assigned by user
`HTTP port has changed to default port.`	An administrator changed the port number for HTTP back to the default (80).
`SSH port has been changed to port %s.`	An administrator changed the port number for SSH. %s is port number assigned by user
`SSH port has been changed to default port.`	An administrator changed the port number for SSH back to the default (22).
`SSH certificate:%s does not exist. SSH service will not work.`	An administrator assigned a nonexistent certificate to SSH. %s is certificate name assigned by user
`SSH certificate:%s format is wrong. SSH service will not work.`	After an administrator assigns a certificate for SSH, the device needs to convert it to a key used for SSH. %s is certificate name assigned by user

Table 325 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`TELNET port has been changed to port %s.`	An administrator changed the port number for TELNET. %s is port number assigned by user
`TELNET port has been changed to default port.`	An administrator changed the port number for TELNET back to the default (23).
`FTP certificate:%s does not exist.`	An administrator assigned a nonexistent certificate to FTP. %s is certificate name assigned by user
`FTP port has been changed to port %s.`	An administrator changed the port number for FTP. %s is port number assigned by user
`FTP port has been changed to default port.`	An administrator changed the port number for FTP back to the default (21).
`SNMP port has been changed to port %s.`	An administrator changed the port number for SNMP. %s is port number assigned by user
`SNMP port has been changed to default port.`	An administrator changed the port number for SNMP back to the default (161).
`Console baud has been changed to %s.`	An administrator changed the console port baud rate. %s is baud rate assigned by user
`Console baud has been reset to %d.`	An administrator changed the console port baud rate back to the default (115200). %d is default baud rate
`DHCP's DNS option:%s has changed.`	DHCP pool's DNS option support from WAN interface. If this interface is unlink/disconnect or link/connect, this log will be shown. %s is interface name. The DNS option of DHCP pool has retrieved from it
`Set timezone to %s.`	An administrator changed the time zone. %s is time zone value
`Set timezone to default.`	An administrator changed the time zone back to the default (0).
`Enable daylight saving.`	An administrator turned on daylight saving.
`Disable daylight saving.`	An administrator turned off daylight saving.
`DNS access control rules have been reached the maximum number.`	An administrator tried to add more than the maximum number of DNS access control rules (64).
`DNS access control rule %u of DNS has been appended.`	An administrator added a new rule. %u is rule number
`DNS access control rule %u has been inserted.`	An administrator inserted a new rule. %u is rule number

Table 325 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`DNS access control rule %u has been appended`	An administrator appended a new rule. %u is rule number
`DNS access control rule %u has been modified`	An administrator modified the rule %u. %u is rule number
`DNS access control rule %u has been deleted.`	An administrator removed the rule %u. %u is rule number
`DNS access control rule %u has been moved to %d.`	An administrator moved the rule %u to index %d. %u is previous index %d variable is current index
`The default record of Zone Forwarder have reached the maximum number of 128 DNS servers.`	The default record DNS servers is more than 128.
`Interface %s ping check is successful. Zone Forwarder adds DNS servers in records.`	Ping check ok, add DNS servers in bind. %s is interface name
`Interface %s ping check is failed. Zone Forwarder removes DNS servers in records.`	Ping check failed, remove DNS servers from bind. %s is interface name
`Interface %s ping check is disabled. Zone Forwarder adds DNS servers in records.`	Ping check disabled, add DNS servers in bind. %s is interface name
`Wizard apply DNS server failed.`	Wizard apply DNS server failed.
`Wizard adds DNS server %s failed because DNS zone setting has conflictd.`	Wizard apply DNS server failed because DNS zone conflicted. %s is the IP address of the DNS server
`Wizard adds DNS server %s failed because Zone Forwarder numbers have reached the maximum number of 32.`	Wizard apply DNS server fail because the device already has the maximum number of DNS records configured. %s is IP address of the DNS server.
`Access control rules of %s have reached the maximum number of %u`	The maximum number of allowable rules has been reached. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. %u is the maximum number of access control rules.

Table 325 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`Access control rule %u of %s was appended.`	A new built-in service access control rule was appended. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was inserted.`	An access control rule was inserted successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was modified.`	An access control rule was modified successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was deleted.`	An access control rule was removed successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %d of %s was moved to %d.`	An access control rule was moved successfully. 1st %d is the previous index . %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. 2nd %d is current previous index.
`SNMP trap can not be sent successfully`	Cannot send a SNMP trap to a remote host due to network error

Table 326 System Logs

LOG MESSAGE	DESCRIPTION
`Port %d is up!!`	When LINK is up, %d is the port number.
`Port %d is down!!`	When LINK is down, %d is the port number.
`%s is dead at %s`	A daemon (process) is gone (was killed by the operating system). 1st %s: Daemon Name, 2nd %s: date and time
`%s process count is incorrect at %s`	The count of the listed process is incorrect. 1st %s: Daemon Name, 2nd %s: date and time
`%s becomes Zombie at %s`	A process is present but not functioning. 1st %s: Daemon Name, 2nd %s: date and time When memory usage exceed threshold-max, memory usage reaches %d%% :mem-threshold-max. When local storage usage exceeds threshold-max, %s: Partition name file system usage reaches %d%%: disk-threshold-max. When memory usage drops below threshold-min, System Memory usage drops below the threshold of %d%%: mem-threshold-min. When local storage usage drops below threshold-min, %s: partition_name file system drops below the threshold of %d%%: disk-threshold-min.

Table 326 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`DHCP Server executed with cautious mode enabled`	DHCP Server executed with cautious mode enabled.
`DHCP Server executed with cautious mode disabled`	DHCP Server executed with cautious mode disabled.
`Received packet is not an ARP response packet`	A packet was received but it is not an ARP response packet.
`Receive an ARP response`	The device received an ARP response.
`Receive ARP response from %s (%s)`	The device received an ARP response from the listed source.
`The request IP is: %s, sent from %s`	The device accepted a request.
`Received ARP response NOT for the request IP address`	The device received an ARP response that is NOT for the requested IP address.
`Receive an ARP response from the client issuing the DHCP request`	The device received an ARP response from the client issuing the DHCP request.
`Receive an ARP response from an unknown client`	The device received an ARP response from an unknown client.
`In total, received %d arp response packets for the requested IP address`	The device received the specified total number of ARP response packets for the requested IP address.
`Clear arp cache successfully.`	The ARP cache was cleared successfully.
`Client MAC address is not an Ethernet address`	A client MAC address is not an Ethernet address.
`DHCP request received via interface %s (%s:%s), src_mac: %s with requested IP: %s`	The device received a DHCP request through the specified interface.
`IP confliction is detected. Send back DHCP-NAK.`	IP conflict was detected. Send back DHCP-NAK.
`Clear ARP cache done`	Clear ARP cache done.
`Set manual time has succeeded. Current time is %s`	The device date and time was changed manually. %s is the date and time.
`NTP update successful, current time is %s`	The device successfully synchronized with a NTP time server . %s is the date and time.

Table 326 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`NTP update failed`	The device was not able to synchronize with the NTP time server successfully.
`Device is rebooted by administrator!`	An administrator restarted the device.
`Insufficient memory.`	Cannot allocate system memory.
`Connect to dyndns server has failed.`	Cannot connect to members.dyndns.org to update DDNS.
`Update the profile %s has failed because of strange server response.`	Update profile failed because the response was strange, %s is the profile name.
`Update the profile %s has succeeded because the IP address of FQDN %s was not changed.`	Update profile succeeded, because the IP address of profile is unchanged, %s is the profile name.
`Update the profile %s has succeeded.`	Update profile succeeded, %s is the profile name.
`Update the profile %s has failed because the FQDN %s is invalid.`	Update profile failed because FQDN for the profile is invalid for DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s is malformed.`	The FQDN format is malformed for DynDNS server, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s is not under your control.`	The owner of this FQDN is not the user, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s was blocked for abuse.`	The FQDN is blocked by DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because of authentication fail.`	Try to update profile, but failed, because of authentication fail, %s is the profile name.
`Update the profile %s has failed because of invalid system parameters.`	Some system parameters are invalid to update FQDN, %s is the profile name.
`Update the profile %s has failed because the FQDN %s was blocked.`	The FQDN is blocked by DynDNS , 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because too many or too few hosts found.`	%s is the profile name.
`Update the profile %s has failed because of dyndns internal error`	Update profile failed because of a dynsdns internal error, %s is the profile name.

Table 326 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`Update the profile %s has failed because the feature requested is only available to donators.`	Update profile failed because the feature requested is only available to donators, %s is the profile name.
`Update the profile %s has failed because of error response.`	Update profile failed because the response is incorrect, %s is the profile name.
`Update the profile %s has failed because %s.`	Update profile failed, and show the response message, 1st %s is the profile name, 2nd %s is the reason.
`Update the profile %s has failed because of unknown error.`	Update profile failed because unknown error. Sometimes, the force authentication will result in this error, 1st %s is the profile name.
`Update the profile %s has failed because Username was empty.`	DDNS profile needs username, %s is the profile name.
`Update the profile %s has failed because Password was empty.`	DDNS profile needs password, %s is the profile name.
`Update the profile %s has failed because Domain name was empty.`	DDNS profile needs domain name, %s is the profile name.
`Update the profile %s has failed because Custom IP was empty.`	The DDNS profile's IP select type is custom, and a custom IP was not defined, %s is the profile name.
`Update the profile %s has failed because WAN interface was empty.`	If the DDNS profile's IP select type is iface, it needs a WAN iface, %s is the profile name.
`Update the profile %s has failed because WAN interface was link-down.`	DDNS profile cannot be updated for WAN IP because WAN iface is link-down, %s is the profile name.
`Update the profile %s has failed because WAN interface was not connected.`	DDNS profile cannot be updated for WAN IP because WAN iface is PPP and not connected, %s is the profile name.
`Update the profile %s has failed because IP address of WAN interface was empty.`	DDNS profile cannot be updated because the IP of WAN iface is 0.0.0.0, 1st %s is the profile name.
`Update the profile %s has failed because ping-check of WAN interface has failed.`	DDNS profile cannot be updated because the ping-check for WAN iface failed , %s is the profile name.
`Disable DDNS has succeeded.`	Disable DDNS.
`Enable DDNS has succeeded.`	Enable DDNS.

Table 326 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`DDNS profile %s has been renamed as %s.`	Rename DDNS profile, 1st %s is the original profile name, 2nd %s is the new profile name.
`DDNS profile %s has been deleted.`	Delete DDNS profile, %s is the profile name,
`DDNS Initialization has failed.`	Initialize DDNS failed,
`All DDNS profiles are deleted`	All DDNS profiles have been removed.
`Collect Diagnostic Information has failed - Server did not respond.`	There was an error and the diagnostics were not completed.
`Collect Diagnostic Infomation has succeeded.`	The diagnostics scripts were executed successfully.
`Port %d is up!!`	The specified port has it’s link up.
`Port %d is down!!`	The specified port has it’s link down.
`Release interface %s failed for packet capture.`	Releasing of the specified interface’s usage count failed while exiting the packet capture function.
`Release address-object %s failed for packet capture.`	Releasing of the specified address object‘s usage count failed while exiting the packet capture function.
`The interface %s is inactive, packet capture for this interface will not take effect.`	The specified interface is not activated so the packet capture for the interface will not take effect.
`Directory packet_trace not existed. Create it automatically.`	The packet trace did not exist so the ISG50 created it automatically.
`Directory debug not existed! Create it automatically.`	A debug directory did not exist so the ISG50 created it automatically.

Table 327 Connectivity Check Logs

LOG MESSAGE	DESCRIPTION
`Can't open link_up2`	Cannot recover routing status which is link-down.
`Can not open %s.pid`	Cannot open connectivity check process ID file. %s: interface name
`Can not open %s.arg`	Cannot open configuration file for connectivity check process. %s: interface name

Table 327 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
`The connectivity-check is activate for %s interface`	The link status of interface is still activate after check of connectivity check process. %s: interface name
`The connectivity-check is fail for %s interface`	The link status of interface is fail after check of connectivity check process. %s: interface name
`Can't get gateway IP of %s interface`	The connectivity check process can't get the gateway IP address for the specified interface. %s: interface name
`Can't alloc memory`	The connectivity check process can't get memory from OS.
`Can't load %s module`	The connectivity check process can't load module for check link-status. %s: the connectivity module, currently only ICMP available.
`Can't handle 'isalive' function of %s module`	The connectivity check process can't execute 'isalive' function from module for check link-status. %s: the connectivity module, currently only ICMP available.
`Create socket error`	The connectivity check process can't get socket to send packet.
`Can't get IP address of %s interface`	The connectivity check process can't get IP address of interface. %s: interface name.
`Can't get flags of %s interface`	The connectivity check process can't get interface configuration. %s: interface name
`Can't get remote address of %s interface`	The connectivity check process can't get remote address of PPP interface %s: interface name
`Can't get NETMASK address of %s interface`	The connectivity check process can't get netmask address of interface. %s: interface name
`Can't get BROADCAST address of %s interface`	The connectivity check process can't get broadcast address of interface %s: interface name
`Can't use MULTICAST IP for destination`	The connectivity check process can't use multicast address to check link-status.
`The destination is invalid, because destination IP is broadcast IP`	The connectivity check process can't use broadcast address to check link-status.
`Can't get MAC address of %s interface!`	The connectivity check process can't get MAC address of interface. %s: interface name
`To send ARP REQUEST error!`	The connectivity check process can't send ARP request packet.
`The %s routing status seted to DEAD by connectivity-check`	The interface routing can't forward packet. %s: interface name

Table 327 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
`The %s routing status seted ACTIVATE by connectivity-check`	The interface routing can forward packet. %s: interface name
`The link status of %s interface is inactive`	The specified interface failed a connectivity check.

Table 328 Routing Protocol Logs

LOG MESSAGE	DESCRIPTION
`RIP on all interfaces have been stopped`	Got the CLI command 'no router rip' to shut down RIP on all interfaces
`Invalid RIP md5 authentication`	RIP md5 authentication has been set without setting md5 authentication id and key first
`Invalid RIP text authentication.`	RIP text authentication has been set without setting authentication key first
`RIP on interface %s has been activated.`	RIP on interface %s has been activated. %s: Interface Name
`RIP direction on interface %s has been changed to In-Only.`	RIP direction on interface %s has been changed to In-Only. %s: Interface Name
`RIP direction on interface %s has been changed to Out-Only.`	RIP direction on interface %s has been changed to Out-Only. %s: Interface Name
`RIP authentication mode has been changed to %s.`	RIP authentication mode has been changed to text or md5.
`RIP text authentication key has been changed.`	RIP text authentication key has been changed.
`RIP md5 authentication id and key have been changed.`	RIP md5 authentication id and key have been changed.
`RIP global version has been changed to %s.`	RIP global version has been changed to version 1 or 2.
`RIP redistribute OSPF routes has been enabled.`	RIP redistribute OSPF routes has been enabled.
`RIP redistribute static routes has been enabled.`	RIP redistribute static routes has been enabled.
`RIP on interface %s has been deactivated.`	RIP on interface %s has been deactivated. %s: Interface Name
`RIP direction on interface %s has been changed to BiDir.`	RIP direction on interface %s has been changed to BiDir. %s: Interface Name
`RIP authentication has benn disabled.`	RIP text or md5 authentication has been disabled.

Table 328 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
`RIP text authentication key has been deleted.`	RIP text authentication key has been deleted.
`RIP md5 authentication id and key have been deleted.`	RIP md5 authentication id and key have been deleted.
`RIP global version has been deleted.`	RIP global version has been deleted.
`RIP redistribute OSPF routes has been disabled.`	RIP redistribute OSPF routes has been disabled.
`RIP redistribute static routes has been disabled.`	RIP redistribute static routes has been disabled.
`RIP v2-broadcast on interface %s has been enabled.`	RIP v2-broadcast on interface %s has been enabled. %s: Interface Name.
`RIP send-version on interface %s has been changed to %s.`	RIP send-version on interface %s has been changed to version 1 or 2 or both 1 2. %s: Interface Name.
`RIP receive-version on interface %s has been changed to %s.`	RIP receive-version on interface %s has been changed to version 1 or 2 or both 1 2. 2nd%s: Interface Name.
`RIP send-version on interface %s has been reset to current global version %s.`	RIP send-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP Version
`RIP receive-version on interface %s has been reset to current global version %s.`	RIP receive-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP
`RIP v2-broadcast on interface %s has been disabled.`	RIP v2-broadcast on interface %s has been disabled. %s: Interface Name
`Area %s cannot be removed. This area is in use.`	One or more interfaces are still using this area, so area %s cannot be removed. %s: OSPF Area
`Invalid OSPF %s authentication of area %s.`	OSPF md5 or text authentication has been set without setting md5 authentication id and key, or text authentication key first.
`Invalid OSPF virtual-link %d md5 authentication of area %s.`	Virtual-link %s md5 authentication has been set without setting md5 authentication id and key first. %s: Virtual-Link ID
`Invalid OSPF virtual-link %s text authentication of area %s.`	Virtual-link %s text authentication has been set without setting text authentication key first. %s: Virtual-Link ID

Table 328 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
`Invalid OSPF virtual-link %s authentication of area %s.`	Virtual-link %s authentication has been set to same-as-area but the area has invalid authentication configuration. %s: Virtual-Link ID
`Invalid OSPF md5 authentication on interface %s.`	Invalid OSPF md5 authentication is set on interface %s. %s: Interface Name
`Invalid OSPF text authentication on interface %s.`	Invalid OSPF text authentication is set on interface %s. %s: Interface Name
`Interface %s does not belong to any OSPF area.`	Interface %s has been set OSPF authentication same-as-area, however the interface does not belong to any OSPF area. %s: Interface Name
`Invalid OSPF authentication of area %s on interface %s.`	Interface %s has been set OSPF authentication same-as-area, however the area has invalid text authentication configuration. %s: Interface Name

Table 329 NAT Logs

LOG MESSAGE	DESCRIPTION
`The NAT range is full`	The NAT mapping table is full.
`%s FTP ALG has succeeded.`	The FTP Application Layer Gateway (ALG) has been turned on or off. %s: Enable or Disable
`Extra signal port of FTP ALG has been modified.`	Extra FTP ALG port has been changed.
`Signal port of FTP ALG has been modified.`	Default FTP ALG port has been changed.
`%s H.323 ALG has succeeded.`	The H.323 ALG has been turned on or off. %s: Enable or Disable
`Extra signal port of H.323 ALG has been modified.`	Extra H.323 ALG port has been changed.
`Signal port of H.323 ALG has been modified.`	Default H.323 ALG port has been changed.
`Register H.323 ALG extra port=%d failed.`	H323 ALG apply additional signal port failed. %d: Port number
`Register H.323 ALG signal port=%d failed.`	H323 ALG apply signal port failed. %d: Port number
`Register FTP ALG extra port=%d failed.`	FTP ALG apply additional signal port failed. %d: Port number
`Register FTP ALG signal port=%d failed.`	FTP ALG apply signal port failed. %d: Port number

Table 330 PKI Logs

LOG MESSAGE	DESCRIPTION
`Generate X509certifiate "%s" successfully`	The router created an X509 format certificate with the specified name.
`Generate X509 certificate "%s" failed, errno %d`	The router was not able to create an X509 format certificate with the specified name. See Table 331 on page 816 for details about the error number.
`Generate certificate request "%s" successfully`	The router created a certificate request with the specified name.
`Generate certificate request "%s" failed, errno %d`	The router was not able to create a certificate request with the specified name. See Table 331 on page 816 for details about the error number.
`Generate PKCS#12 certificate "%s" successfully`	The router created a PKCS#12 format certificate with the specified name.
`Generate PKCS#12 certificate "%s" failed, errno %d`	The router was not able to create anPKCS#12 format certificate with the specified name. See Table 331 on page 816 for details about the error number.
`Prepare to import "%s" into "My Certificate"`	%s is the name of a certificate request.
`Prepare to import "%s" into Trusted Certificate"`	%s is the name of a certificate request.
`CMP enrollment "%s" successfully, CA "%s", URL "%s"`	The device used CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
`CMP enrollment "%s" failed, CA "%s", URL "%s"`	The device was unable to use CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
`SCEP enrollment "%s" successfully, CA "%s", URL "%s"`	The device used SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
`SCEP enrollment "%s" failed, CA "%s", URL "%s"`	The device was unable to use SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
`Import X509 certificate "%s" into My Certificate successfully`	The device imported a x509 format certificate into My Certificates. %s is the certificate request name.
`Import X509 certificate "%s" into Trusted Certificate successfully`	The device imported a x509 format certificate into Trusted Certificates. %s is the certificate request name.
`Import PKCS#12 certificate "%s" into "My Certificate" successfully`	The device imported a PKCS#12 format certificate into My Certificates. %s is the certificate request name.

Table 330 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Import PKCS#7 certificate "%s" into "My Certificate" successfully`	The device imported a PKCS#7 format certificate into My Certificates. %s is the certificate request name.
`Import PKCS#7 certificate "%s" into "Trusted Certificate" successfully`	The device imported a PKCS#7 format certificate into Trusted Certificates. %s is the certificate request name.
`Decode imported certificate "%s" failed`	The device was not able to decode an imported certificate. %s is certificate the request name
`Export PKCS#12 certificate "%s" from "My Certificate" successfully`	The device exported a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
`Export PKCS#12 certificate "%s" from "My Certificate" failed`	The device was not able to export a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "My Certificate" failed`	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "Trusted Certificate" failed`	The device was not able to export a x509 format certificate from Trusted Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "My Certificate" successfully`	The device exported a x509 format certificate from My Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "Trusted Certificate" successfully`	The device exported a x509 format certificate from Trusted Certificates. %s is the certificate request name.
`Export X509 certificate "%s" from "My Certificate" failed`	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
`Import PKCS#12 certificate "%s" with incorrect password`	An administrator used the wrong password when trying to import a PKCS#12 format certificate. %s is the certificate name.
`Cert trusted: %s`	%s is the subject.
`Due to %d, cert not trusted: %s`	%d is an error number (see Table 331 on page 816), %s is the certificate subject.

Table 331 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 332 Interface Logs

LOG MESSAGE	DESCRIPTION
`Interface %s has been deleted.`	An administrator deleted an interface. %s is the interface name.
`Create interface %s has been failed.`	When PPP can't running fail, %s: interface name.
`Base interface %s is disabled. Interface %s is disabled now.`	When user disable ethernet, vlan or bridge interface and this interface is base interface of PPP or virtual interface. PPP and virtual will disable too. 1st %s is interface name, 2nd %s is interface.
`Interface %s has been changed.`	An administrator changed an interface's configuration. %s: interface name.

Table 332 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`Interface %s has been added.`	An administrator added a new interface. %s: interface name.
`Interface %s is enabled.`	An administrator enabled an interface. %s: interface name.
`Interface %s is disabled.`	An administrator disabled an interface. %s: interface name.
`%s MTU > (%s MTU - 8), %s may not work correctly.`	An administrator configured a PPP interface, PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and the peer will not receive correct PPP packets. 1st %s: PPP interface name, 2nd %s: ethernet interface name.
`(%s MTU - 8) < %s MTU, %s may not work correctly.`	An administrator configured ethernet, vlan or bridge and this interface is base interface of PPP interface. PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and peer will not receive correct PPP packets.1st %s: Ethernet interface name, 2nd %s: PPP interface name.
`Interface %s links down. Default route will not apply until interface %s links up.`	An administrator set a static gateway in interface but this interface is link down. At this time the configuration will be saved but route will not take effect until the link becomes up.1st %s: interface name, 2nd %s: interface name.
`name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u,UpTime=%s`	Port statistics log. This log will be sent to the VRPT server. 1st %s: physical port name, 2nd %s: physical port status, 1st %u: physical port Tx packets, 2nd %u: physical port Rx packets, 3rd %u: physical port packets collisions, 4th %u: physical port Tx Bytes/s, 5th %u: physical port Rx Bytes/s, 3rd %s: physical port up time.
`name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u`	Interface statistics log. This log will be sent to the VRPT server. 1st %s: interface name, 2nd %s: interface status, 1st %u variable: interface Tx packets, 2nd %u variable: interface Rx packets, 3rd %u: interface packets collisions, 4th %u: interface Tx Bytes/s, 5th %u: interface Rx Bytes/s.
`Interface %s start dailing.`	A PPP interface started dialing to a server. %s: interface name.
`Interface %s connect failed: Connect to server failed.`	A PPTP interface failed to connect to the PPTP server. %s: interface name.
`Interface %s connection terminated.`	A PPP connection will terminate. %s: interface name.
`Interface %s connection terminated: idle timeout.`	An idle PPP connection timed out.1%s: interface name.
`Interface %s connect failed: MS-CHAPv2 mutual authentication failed.`	MS-CHAPv2 authentication failed (the server must support mS-CHAPv2 and verify that the authentication failed, this does not include cases where the servers does not support MS-CHAPv2). %s: interface name.

Table 332 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`Interface %s connect failed: MS-CHAP authentication failed.`	MS-CHAP authentication failed (the server must support MS-CHAP and verify that the authentication failed, this does not include cases where the server does not support MS-CHAP). %s: interface name.
`Interface %s connect failed: CHAP authentication failed.`	CHAP authentication failed (the server must support CHAP and verify that the authentication failed, this does not include cases where the server does not support CHAP). CHAP: interface name.
`Interface %s is connected.`	A PPP interface connected successfully. %s: interface name.
`Interface %s is disconnected.`	A PPP interface disconnected successfully. %s: interface name.
`Interface %s connect failed: Peer not responding.`	The interface's connection will be terminated because the server did not send any LCP packets. %s: interface name.
`Interface %s connect failed: PAP authentication failed.`	PAP authentication failed (the server must support PAP and verify verify that the authentication failed, this does not include cases where the server does not support PAP). %s: PPP interface name.
`Interface %s connect failed: Connect timeout.`	A PPPOE connection timed out due to a lack of response from the PPPOE server. %s: PPP interface name.
`Interface %s create failed because has no member.`	A bridge interface has no member. %s: bridge interface name.
`"Interface cellular Application Error Code %d\n.`	The listed error code (%d) was generated due to an internal cellular interface error.
`"An error [%d] occurred while negotiating with the device in %s. Please try to remove then insert the device.`	The listed error code (%d) happened when the ISG50 attempted to negotiate with the cellular device installed in (or connected to) the listed slot (%s). Remove and reinstall the device.
`"Unable to negotiate with the device in %s. Please try to remove then insert the device.`	The ISG50 could not negotiate with the cellular device installed in (or connected to) the listed slot (%s). Remove and reinstall the device.
`"Unable to configure the selected frequency band to the device in %s. Please try to remove then insert the device.`	The ISG50 failed to set the cellular device installed in (or connected to) the listed slot (%s) to use the frequency band you configured. The cellular device may not support the band or you may need to try removing and reinstalling the device.
`"PIN code is required for inteface cellular%d. Please check the PIN code setting.`	The PIN code configured for the listed cellular interface (%d) is incorrect or missing.

Table 332 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`"SIM card has been successfully unlocked by PUK code on interface cellular%d.`	You entered the correct PUK code and unlocked the SIM card for the cellular device associated with the listed cellular interface (%d).
`"Incorrect PUK code of interface cellular%d. Please check the PUK code setting.`	You entered an incorrect PUK code so you were not able to unlock the SIM card for the cellular device associated with the listed cellular interface (%d).
`"SIM card of interface cellular%d in %s is damaged or not inserted. Please remove the device, then check the SIM card.`	The SIM card for the cellular device associated with the listed cellular interface (%d) cannot be detected. The SIM card may be missing, not inserted properly, or damaged. Remove the device and check its SIM card. If it does not appear to be damaged, try re-inserting the SIM card.
`"SIM card of interface cellular%d in %s is locked. Please enter PUK code to unlock.`	The SIM card for the cellular device associated with the listed cellular interface (%d) is locked. This may be because the PIN code was entered incorrectly more than three times. You need to enter the PUK code to unlock the SIM card. .
`"Incorrect PIN code of interface cellular%d. Please check the PIN code setting.`	The listed cellular interface (%d) does has the wrong PIN code configured.
`"Unable to query the signal quality from the device in %s. Please try to remove then insert the device.`	The ISG50 could not check the signal strength for the listed cellular interface (%d). This could be due to an error or being out of range of the ISP's cellular station.
`"Interface cellular%d cannot connect to the service provider.`	The listed cellular interface (%d) cannot connect to the ISP. This could be due to an error or being out of range of the ISP's cellular station.
`"Interface cellular%d is configured with incorrect APN.`	The listed cellular interface (%d) does not have the correct APN (Access Point Name) configured.
`"Interface cellular%d is configured with incorrect phone number.`	The listed cellular interface (%d) does not have the correct phone number configured.
`"Interface cellular%d is configured with incorrect username or password.`	The listed cellular interface (%d) does not have the correct user name and password configured.
`"Interface cellular%d is configured with device %s, but current inserted device is %s.`	The listed cellular interface (%d) is configured for a particular cellular device (first %s), but a different cellular device (second %s) is inserted.
`"Cellular device [%s %s] has been inserted into %s.`	The cellular device (identified by its manufacturer and model) has been inserted in or connected to the specified slot.

Table 332 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`"Cellular device [%s %s] has been removed from %s.`	The cellular device (identified by its manufacturer and model) has been removed from the specified slot.
`Interface cellular%d required authentication password.Please set password in cellular%d edit page.`	You need to manually enter the password for the listed cellular interface (%d).
`"Cellular%d (IMSI=%s or ESN=%s) over time budget!(budget = %d seconds).`	The listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed time budget threshold value (second %d).
`"Cellular%d (IMSI=%s or ESN=%s) over time budget %d%% (budget = %d seconds).`	The listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed percentage of the time budget threshold value (second %d).
`"Cellular%d (IMSI=%s or ESN=%s) over time budget!(budget = %d seconds).`	This alert lets you know that the listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed time budget threshold value (second %d).
`"Cellular%d (IMSI=%s or ESN=%s) over time budget %d%% (budget = %d seconds).`	This alert lets you know that the listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed percentage of the time budget threshold value (second %d).
`"Cellular%d (IMSI=%s or ESN=%s) over data budget!(budget = %lld Mbytes, used = %lld Mbytes).`	The listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed data budget by the listed number of MB.
`"Cellular%d (IMSI=%s or ESN=%s) over data budget %d%% (budget = %.2f Mbytes, used = %.2f Mbytes).`	The listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed percentage of the data budget threshold value.
`"Cellular%d (IMSI=%s or ESN=%s) over data budget!(budget = %lld Mbytes, used = %lld Mbytes).`	This alert lets you know that the listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed data budget by the listed number of MB.
`"Cellular%d (IMSI=%s or ESN=%s) over data budget %d%% (budget = %.2f Mbytes, used = %.2f Mbytes).`	This alert lets you know that the listed cellular interface (%d) with the listed SIM card IMSI number or IMEI/ESN number went over the listed percentage of the data budget threshold value.
`The interface name is not accepted.`	An incorrect name was not permitted for an interface.
`Configured interface name is reserved word.`	A reserved word was not permitted to be used in an interface name.

Table 332 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`Configured interface name match reserved prefix.`	A reserved pre-fix was not permitted to be used in an interface name.
`Duplicated interface name.`	A duplicate name was not permitted for an interface.
`This Interface can not be renamed.`	An interface's name cannot be changed.
`Virtual interface is not supported on this type of interface.`	A virtual interface was not created on an interface because the type of interface does not support virtual interfaces.
`Virtual interface need to be removed before changing the interface property.`	An interface property cannot be changed because the interface has a virtual interface on it.
`Virtual interface can not configured at external interface.`	A virtual interface cannot be configured on an external interface.
`Interface property is not accepted.`	An invalid interface property was not accepted.
`The property can not be changed at this interface.`	An interface property cannot be changed.
`System default ppp interface can not bind with other ethernet interface.`	The system default PPP interface can only be bound with the corresponding Ethernet interface, not any other.
`Related system default ppp interface need to deactivate first.`	The related system default PPP interface has to be deactivated before the attempted configuration can be done.
`Related system default ppp interface can not be activated since interface property is internal.`	The system default PPP interface cannot be activated because it is related to an internal interface.
`System default ppp interface can not be removed.`	A PPP interface could not be removed because it is a system default PPP interface.
`Interface property can not change to internal since interface is the member of other trunk.`	An interface can not be set to be an internal interface because it is a member of a trunk.
`Port-grouping is not support`	The interface does not support port grouping.
`This interface type can not set 3rd-dns.`	This type of interface does not support setting a third DNS server setting.

Table 332 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u,UpTime=%s`	This log is sent to the VRPT server to show the specified PPP/Cellular interface's statistics and uptime. The arguments represent the interface name, interface status, interface Tx packets, interface Rx packets, interface collision packets, interface Tx Bytes/s, interface Rx Bytes/s, and interface up time.
`Interface %s has been renamed from '%s' to '%s '`	The user-configurable name of the specified interface (internal system name) has been renamed from one name to another.

Table 333 Account Logs

LOG MESSAGE	DESCRIPTION
`Account %s %s has been deleted.`	A user deleted an ISP account profile. 1st %s: profile type, 2nd %se: profile name.
`Account %s %s has been changed.`	A user changed an ISP account profile's options. 1st %s: profile type, 2nd %s: profile name.
`Account %s %s has been added.`	A user added a new ISP account profile. 1st %s: profile type, 2nd %s: profile name.

Table 334 Port Grouping Logs

LOG MESSAGE	DESCRIPTION
`Interface %s links up because of changing Port Group. Enable DHCP client.`	An administrator used port-grouping to assign a port to a representative Interface and this representative interface is set to DHCP client and only has one member. In this case the DHCP client will be enabled. %s: interface name.
`Interface %s links down because of changing Port Group. Disable DHCP client.`	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has no members in its group. In this case the DHCP client will be disabled. %s: interface name.
`Port Group on %s is changed. Renew DHCP client.`	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has more than one member in its group. In this case the DHCP client will renew. %s: interface name.
`Port Grouping %s has been changed.`	An administrator configured port-grouping, %s: interface name.

Table 335 Force Authentication Logs

LOG MESSAGE	DESCRIPTION
`Force User Authentication will be enabled due to http server is enabled.`	Force user authentication will be turned on because HTTP server was turned on.
`Force User Authentication will be disabled due to http server is disabled.`	Force user authentication will be turned off because HTTP server was turned off.
`Force User Authentication may not work properly!`	

Table 336 File Manager Logs

LOG MESSAGE	DESCRIPTION
`ERROR:#%s, %s`	Apply configuration failed, this log will be what CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
`WARNING:#%s, %s`	Apply configuration failed, this log will be what CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
`ERROR:#%s, %s`	Run script failed, this log will be what wrong CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
`WARNING:#%s, %s`	Run script failed, this log will be what wrong CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
`Resetting system...`	Before apply configuration file.
`System resetted. Now apply %s..`	After the system reset, it started to apply the configuration file. %s is configuration file name.
`Running %s...`	An administrator ran the listed shell script. %s is script file name.
`Going to rollback previous running-config.`	Applying the configuration file failed and the ISG50 is going to roll back to the previous running-config.

Table 337 DHCP Logs

LOG MESSAGE	DESCRIPTION
Can't find any lease for this client - %s, DHCP pool full!	All of the IP addresses in the DHCP pool are already assigned to DHCP clients, so there is no IP address to give to the listed DHCP client.
DHCP server offered %s to %s(%s)	The DHCP server feature gave the listed IP address to the computer with the listed hostname and MAC address.
Requested %s from %s(%s)	The ISG50 received a DHCP request for the specified IP address from the computer with the listed hostname and MAC address.
No applicable lease found for DHCP request - %s !	There is no matching DHCP lease for a DHCP client's request for the specified IP address.
DHCP released %s with %s(%s)	A DHCP client released the specified IP address. The DHCP client's hostname and MAC address are listed.
Sending ACK to %s	The DHCP server feature received a DHCP client's inform packet and is sending an ACK to the client.
DHCP server assigned %s to %s(%s)	The DHCP server feature assigned a client the IP address that it requested. The DHCP client's hostname and MAC address are listed.

Table 338 E-mail Daily Report Logs

LOG MESSAGE	DESCRIPTION
`Email Daily Report has been activated.`	The daily e-mail report function has been turned on. The ISG50 will e-mail a daily report about the selected items at the scheduled time if the required settings are configured correctly.
`Email Daily Report has been deactivated.`	The daily e-mail report function has been turned off. The ISG50 will not e-mail daily reports.
`Email daily report has been sent successfully.`	The ISG50 sent a daily e-mail report mail successfully.
`Cannot resolve mail server address %s.`	The (listed) SMTP address configured for the daily e-mail report function is incorrect.
`Mail server authentication failed.`	The user name or password configured for authenticating with the e-mail server is incorrect.
`Failed to send report. Mail From address %s1 is inconsistent with SMTP account %s2.`	The user name and password configured for authenticating with the e-mail server are correct, but the (listed) sender e-mail address does not match the (listed) SMTP e-mail account.
`Failed to connect to mail server %s.`	The ISG50 could not connect to the SMTP e-mail server (%s). The address configured for the server may be incorrect or there may be a problem with the ISG50's or the server's network connection.

Table 339 IP-MAC Binding Logs

LOG MESSAGE	DESCRIPTION
Drop packet %s-%u.%u.%u.%u-%02X:%02X:%02X:%02X:%02X:%02X	The IP-MAC binding feature dropped an Ethernet packet. The interface the packet came in through and the sender's IP address and MAC address are also shown.
Cannot bind ip-mac from dhcpd: %s#%u.%u.%u.%u#%02X:%02X:%02X:%02X:%02X:%02X.	The IP-MAC binding feature could not create an IP-MAC binding hash table entry. The interface the packet came in through, the sender's IP address and MAC address, are also shown along with the binding type ("s" for static or "d" for dynamic).
Cannot remove ip-mac binding from dhcpd: %s#%u.%u.%u.%u#%02X:%02X:%02X:%02X:%02X:%02X.	The IP-MAC binding feature could not delete an IP-MAC binding hash table entry. The interface the packet came in through, the sender's IP address and MAC address, are also shown along with the binding type ("s" for static or "d" for dynamic).

Table 340 Auth. Policy Logs

LOG MESSAGE	DESCRIPTION
Auth. Policy featuer is disabled.	The auth. policy feature is not enabled.
Auth. policy %d is disabled.	The specified auth. policy rule is not activated.
System integrity error!	The ISG50 cannot get the auth. policy rule and related operation index.
Get lock id has failed	Cannot get semaphore locked ID.
Lock buffer id has failed	Cannot use the current semaphore related buffer.

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 341 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 341 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SIP	UDP	5060	Session Initiation Protocol.

Table 341 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

C

Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the ISG50, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (🔒) somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

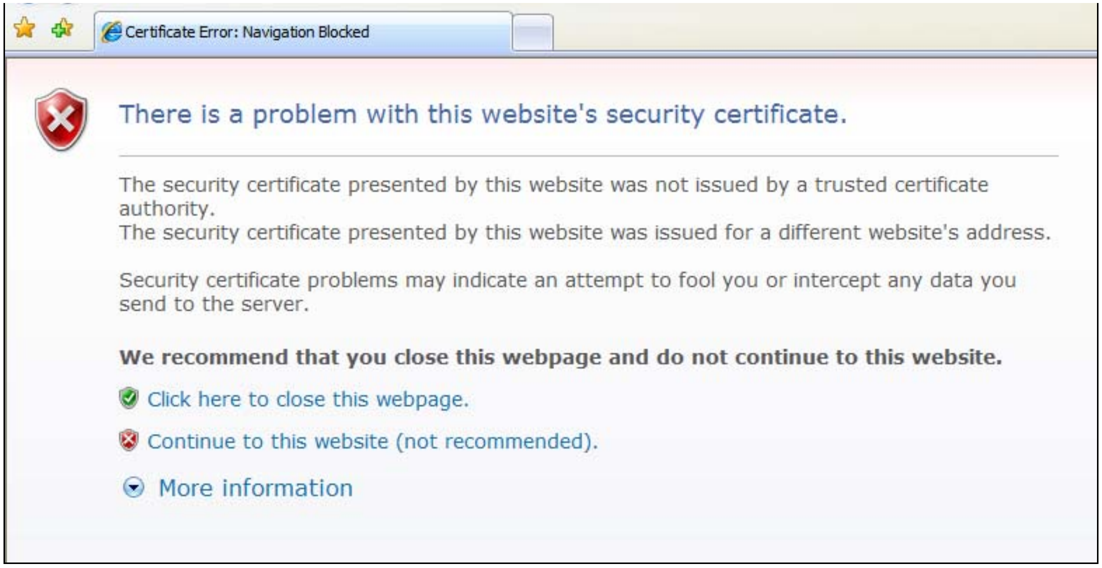
- Internet Explorer on page 831
- Firefox on page 839
- Opera on page 844
- Konqueror on page 850

Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

Figure 530 Internet Explorer 7: Certification Error


Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

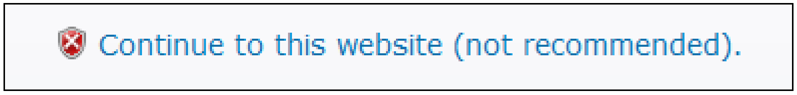
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

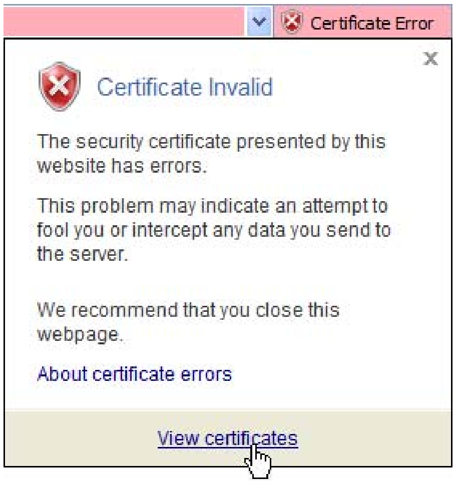
2 Click **Continue to this website (not recommended)**.

Figure 531 Internet Explorer 7: Certification Error


Continue to this website (not recommended).

3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

Figure 532 Internet Explorer 7: Certificate Error


Certificate Error

Certificate Invalid

The security certificate presented by this website has errors.

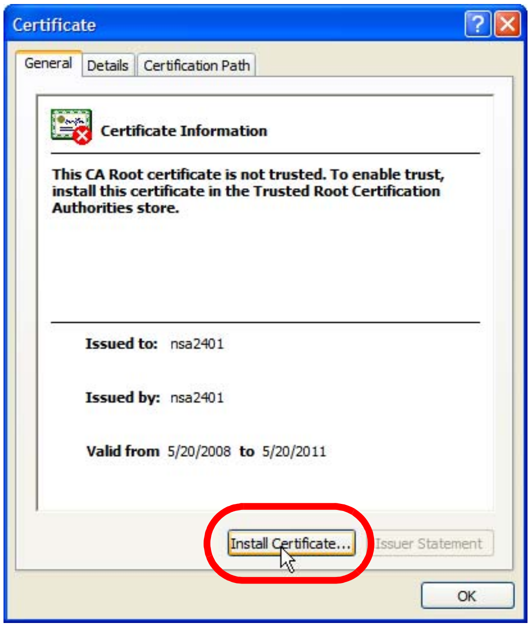
This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors
View certificates

4 In the **Certificate** dialog box, click **Install Certificate**.

Figure 533 Internet Explorer 7: Certificate



Certificate
General
Details
Certification Path
Install Certificate...
Issuer Statement
OK

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

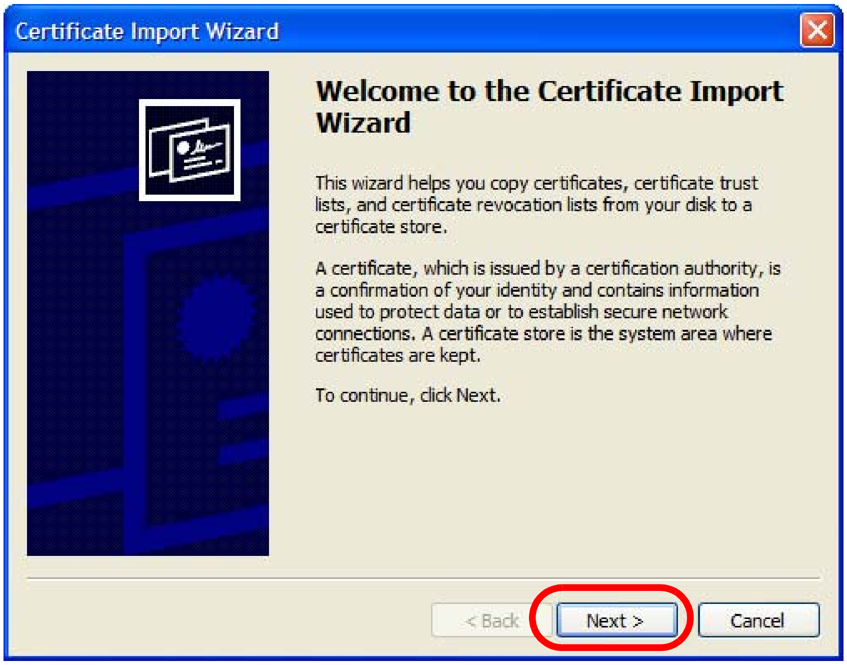
Issued to: nsa2401

Issued by: nsa2401

Valid from 5/20/2008 to 5/20/2011

5 In the **Certificate Import Wizard**, click **Next**.

Figure 534 Internet Explorer 7: Certificate Import Wizard



Certificate Import Wizard
< Back
Next >
Cancel

Welcome to the Certificate Import Wizard

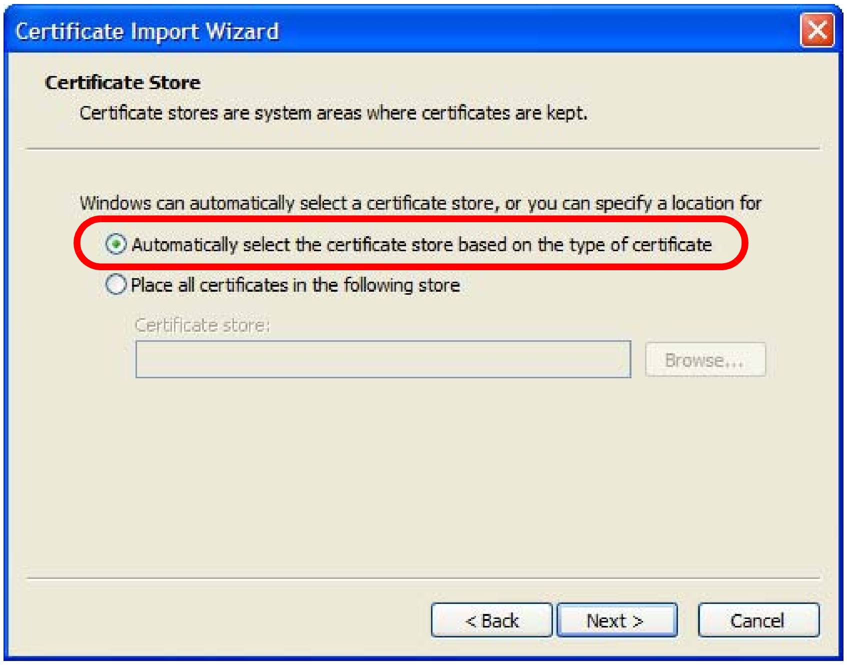
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

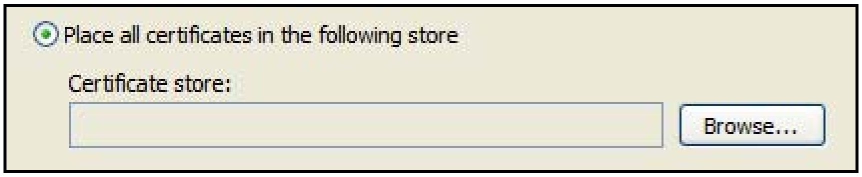
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

Figure 535 Internet Explorer 7: Certificate Import Wizard


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
● Automatically select the certificate store based on the type of certificate
○ Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

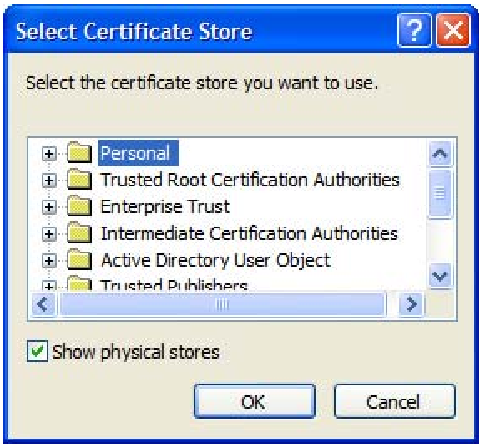
7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

Figure 536 Internet Explorer 7: Certificate Import Wizard


● Place all certificates in the following store
Certificate store:
Browse...

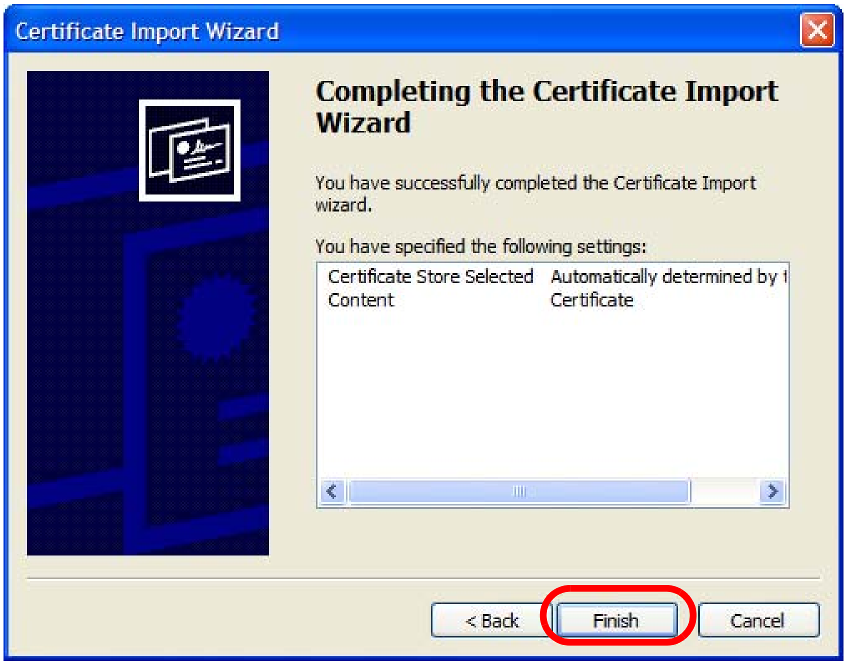
8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 537 Internet Explorer 7: Select Certificate Store


Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
☑ Show physical stores
OK
Cancel

9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 538 Internet Explorer 7: Certificate Import Wizard



Completing the Certificate Import Wizard

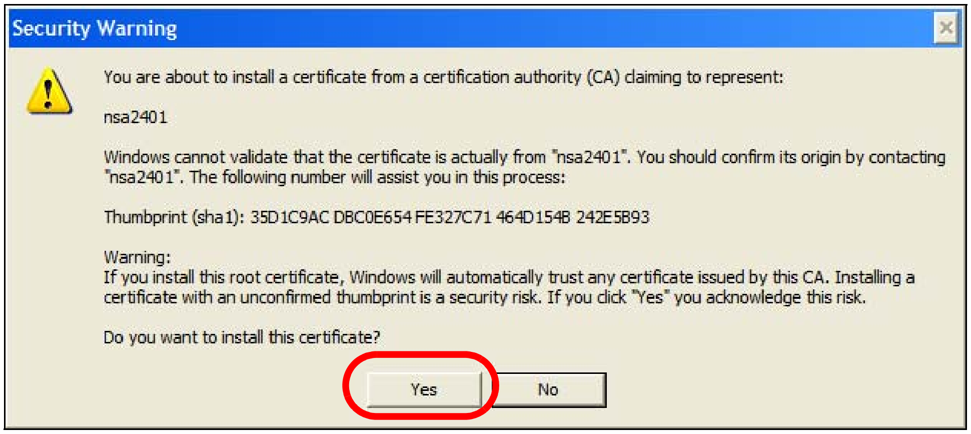
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

10 If you are presented with another **Security Warning**, click **Yes**.

Figure 539 Internet Explorer 7: Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

nsa2401

Windows cannot validate that the certificate is actually from "nsa2401". You should confirm its origin by contacting "nsa2401". The following number will assist you in this process:

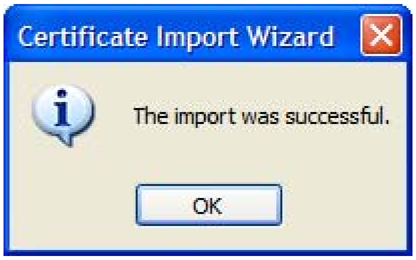
Thumbprint (sha1): 35D1C9AC DBC0E654 FE327C71 464D154B 242E5B93

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

11 Finally, click **OK** when presented with the successful certificate installation message.

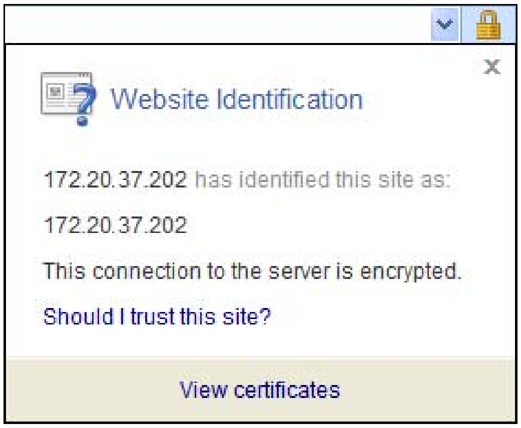
Figure 540 Internet Explorer 7: Certificate Import Wizard



The import was successful.

12 The next time you start Internet Explorer and go to a ZyXEL Web Configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

Figure 541 Internet Explorer 7: Website Identification



Website Identification

172.20.37.202 has identified this site as:

172.20.37.202

This connection to the server is encrypted.

Should I trust this site?

Installing a Stand-Alone Certificate File in Internet Explorer

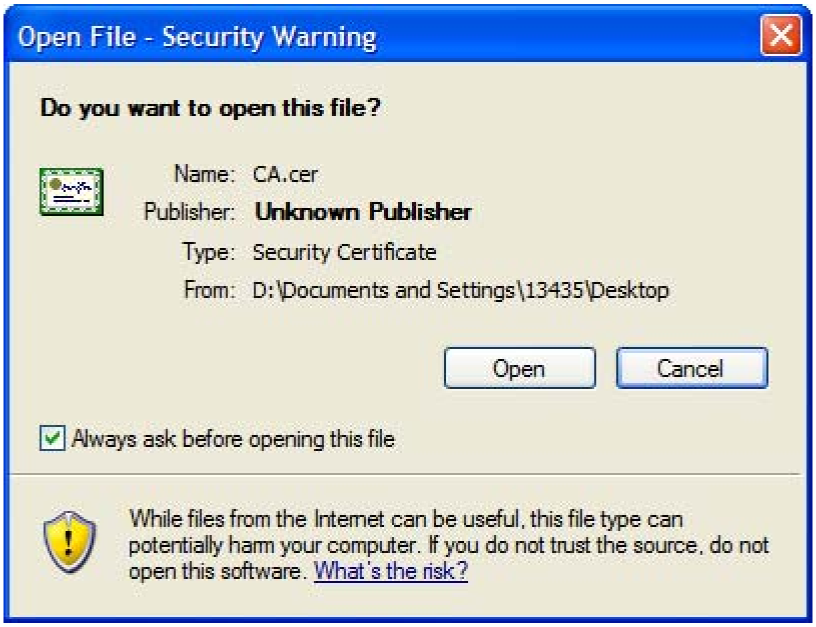
Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 542 Internet Explorer 7: Public Key Certificate File

2 In the security warning dialog box, click **Open**.

Figure 543 Internet Explorer 7: Open File - Security Warning


Open File - Security Warning
Do you want to open this file?
Name: CA.cer
Publisher: Unknown Publisher
Type: Security Certificate
From: D:\Documents and Settings\13435\Desktop
Open
Cancel
☑ Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

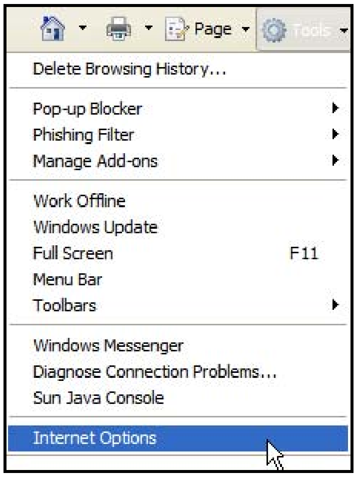
3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 831 to complete the installation process.

Removing a Certificate in Internet Explorer

This section shows you how to remove a public key certificate in Internet Explorer 7.

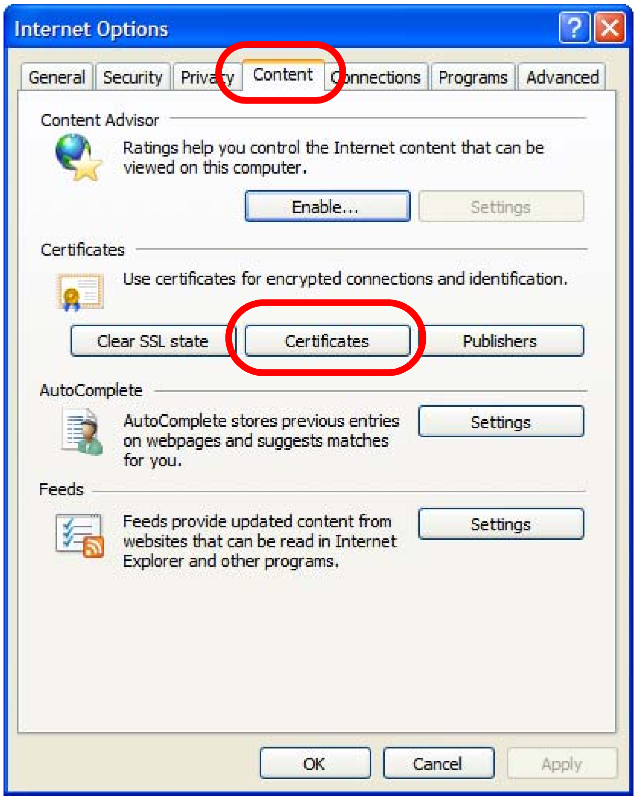
1 Open **Internet Explorer** and click **Tools > Internet Options**.

Figure 544 Internet Explorer 7: Tools Menu


Page
Tools
Delete Browsing History...
Pop-up Blocker
Phishing Filter
Manage Add-ons
Work Offline
Windows Update
Full Screen F11
Menu Bar
Toolbars
Windows Messenger
Diagnose Connection Problems...
Sun Java Console
Internet Options

2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

Figure 545 Internet Explorer 7: Internet Options


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Content Advisor
Enable...
Settings
Certificates
Clear SSL state
Certificates
Publishers
AutoComplete
Settings
Feeds
Settings
OK
Cancel
Apply

Ratings help you control the Internet content that can be viewed on this computer.

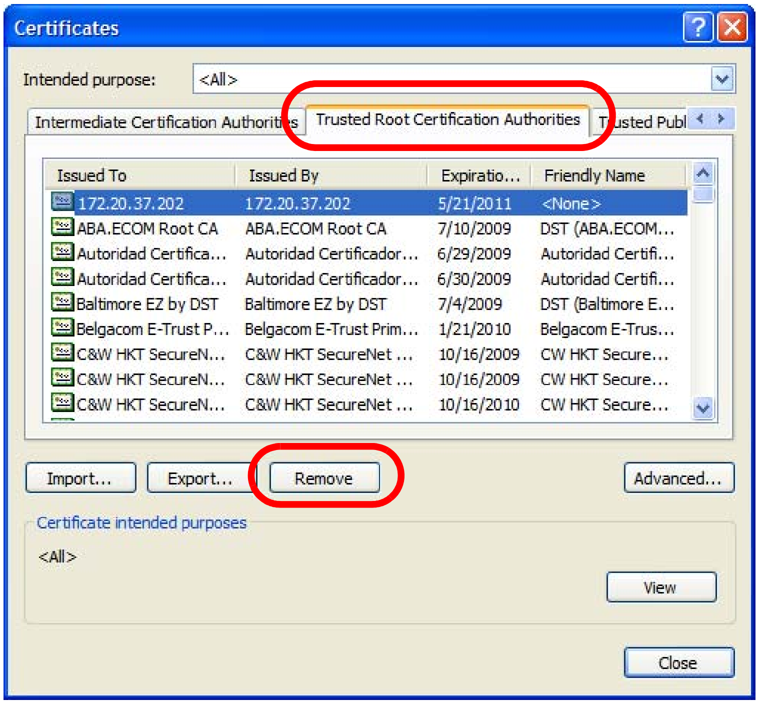
Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

Figure 546 Internet Explorer 7: Certificates


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

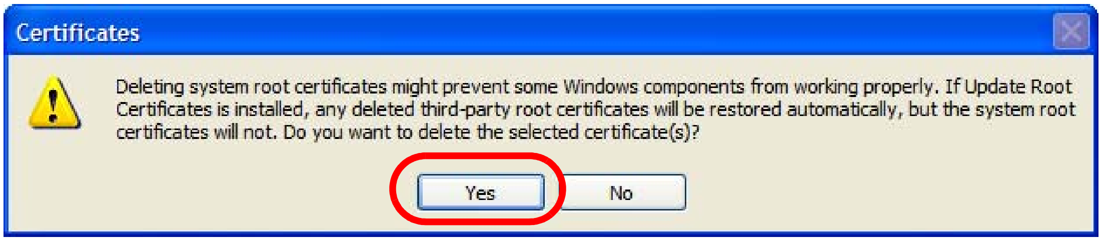
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
172.20.37.202	172.20.37.202	5/21/2011	<None>
ABA.ECOM Root CA	ABA.ECOM Root CA	7/10/2009	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	6/30/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/4/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...

<All>

4 In the **Certificates** confirmation, click **Yes**.

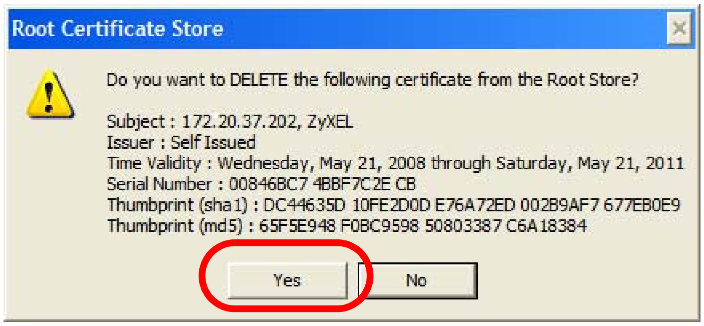
Figure 547 Internet Explorer 7: Certificates



Deleting system root certificates might prevent some Windows components from working properly. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?

5 In the **Root Certificate Store** dialog box, click **Yes**.

Figure 548 Internet Explorer 7: Root Certificate Store



Do you want to DELETE the following certificate from the Root Store?

Subject : 172.20.37.202, ZyXEL
Issuer : Self Issued
Time Validity : Wednesday, May 21, 2008 through Saturday, May 21, 2011
Serial Number : 00846BC7 4BBF7C2E CB
Thumbprint (sha1) : DC44635D 10FE2D0D E76A72ED 002B9AF7 677EB0E9
Thumbprint (md5) : 65F5E948 F0BC9598 50803387 C6A18384

6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

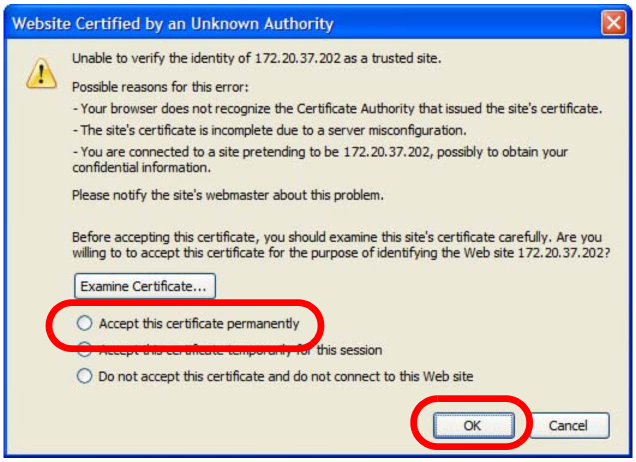
Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

2 Select **Accept this certificate permanently** and click **OK.**

Figure 549 Firefox 2: Website Certified by an Unknown Authority



Unable to verify the identity of 172.20.37.202 as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be 172.20.37.202, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site 172.20.37.202?

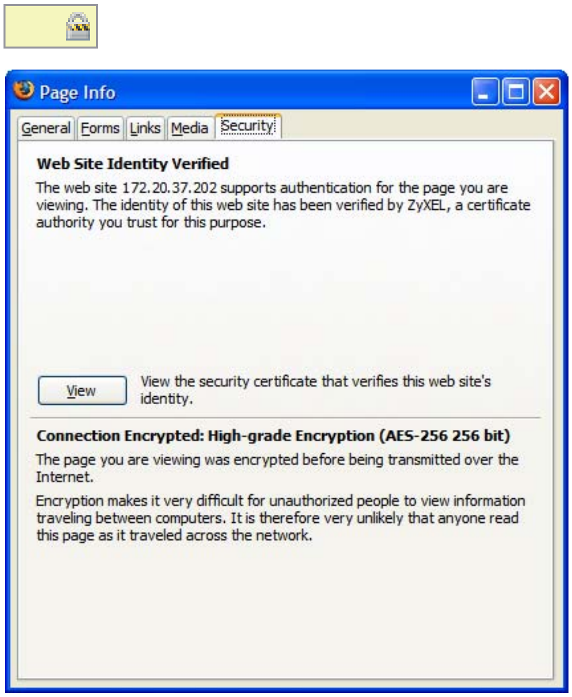
○ Accept this certificate permanently

○ Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

3 The certificate is stored and you can now connect securely to the Web Configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.

Figure 550 Firefox 2: Page Info



Web Site Identity Verified

The web site 172.20.37.202 supports authentication for the page you are viewing. The identity of this web site has been verified by ZyXEL, a certificate authority you trust for this purpose.

View the security certificate that verifies this web site's identity.

Connection Encrypted: High-grade Encryption (AES-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

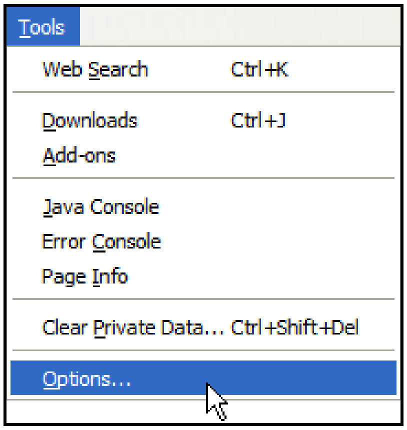
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

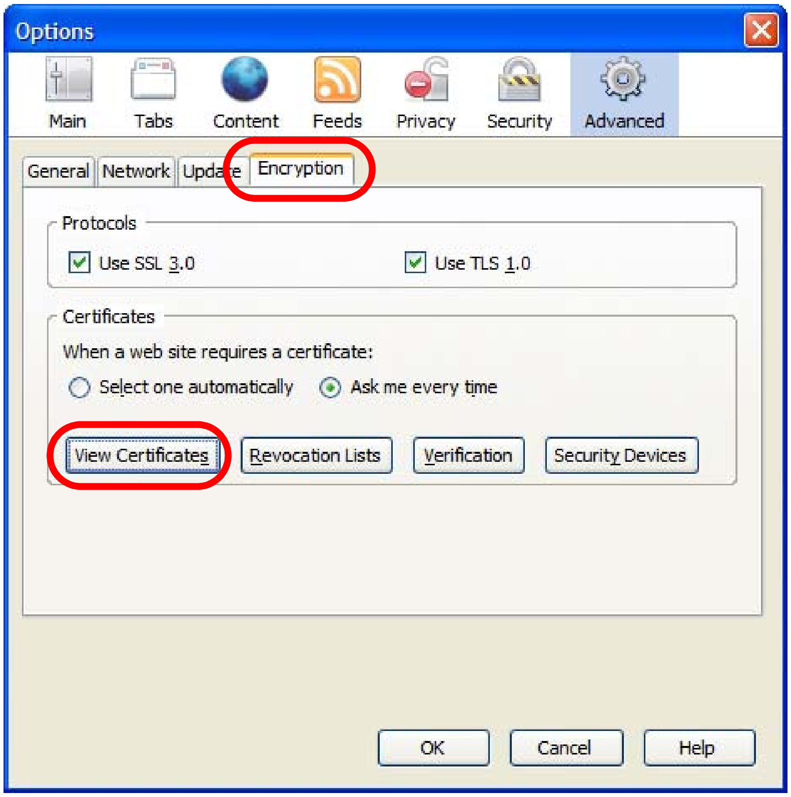
1 Open **Firefox** and click **Tools** > **Options**.

Figure 551 Firefox 2: Tools Menu


Tools
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Java Console
Error Console
Page Info
Clear Private Data... Ctrl+Shift+Del
Options...

2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 552 Firefox 2: Options


Options
Main
Tabs
Content
Feeds
Privacy
Security
Advanced
General
Network
Update
Encryption
Protocols
Certificates
View Certificates
Revocation Lists
Verification
Security Devices
OK
Cancel
Help

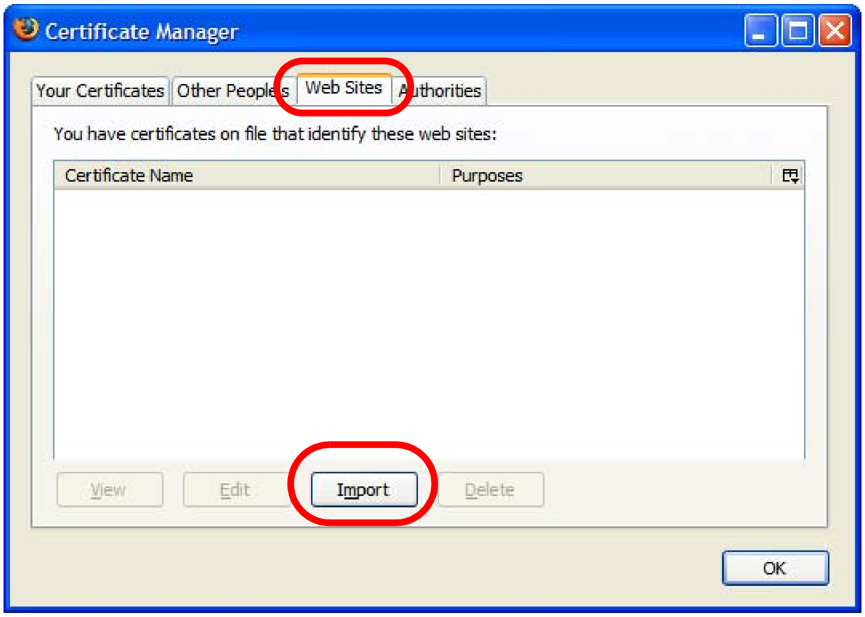
☑ Use SSL 3.0 ☑ Use TLS 1.0

When a web site requires a certificate:

○ Select one automatically ● Ask me every time

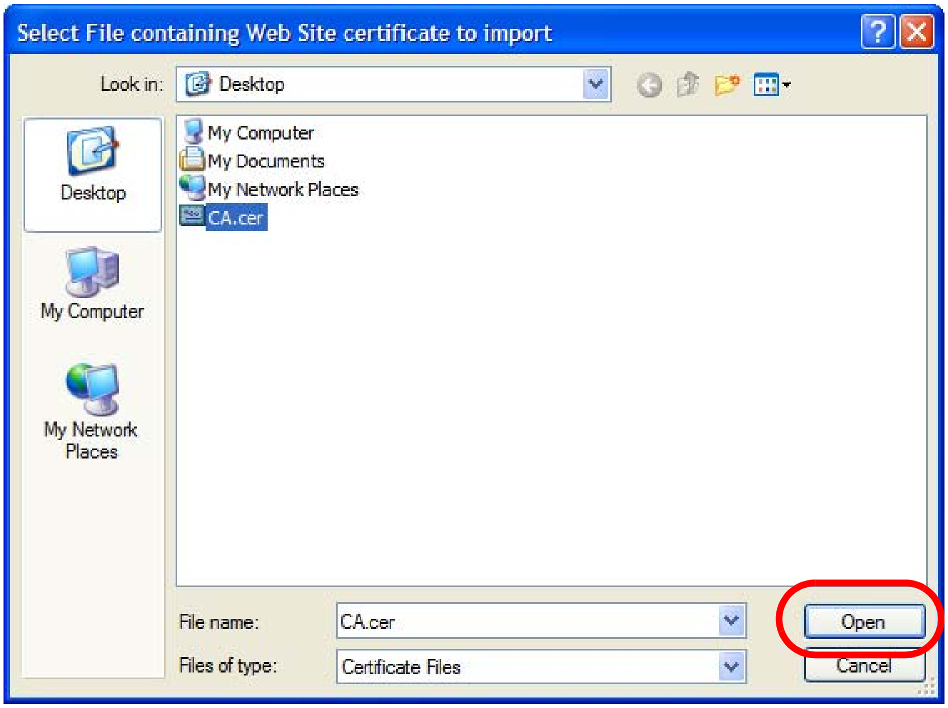
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 553 Firefox 2: Certificate Manager


Certificate Manager
Your Certificates
Other People's
Web Sites
Authorities
You have certificates on file that identify these web sites:
Certificate Name
Purposes
View
Edit
Import
Delete
OK

4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

Figure 554 Firefox 2: Select File


Select File containing Web Site certificate to import
Look in:
Desktop
My Computer
My Documents
My Network Places
CA.cer
Desktop
My Computer
My Network Places
File name:
CA.cer
Files of type:
Certificate Files
Open
Cancel

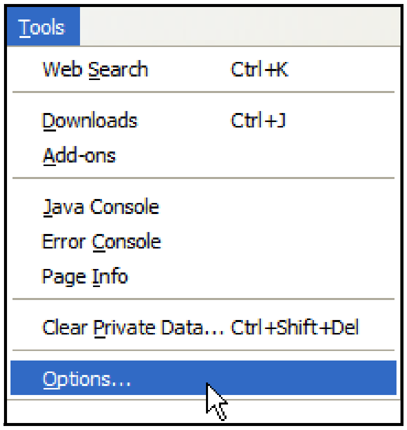
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

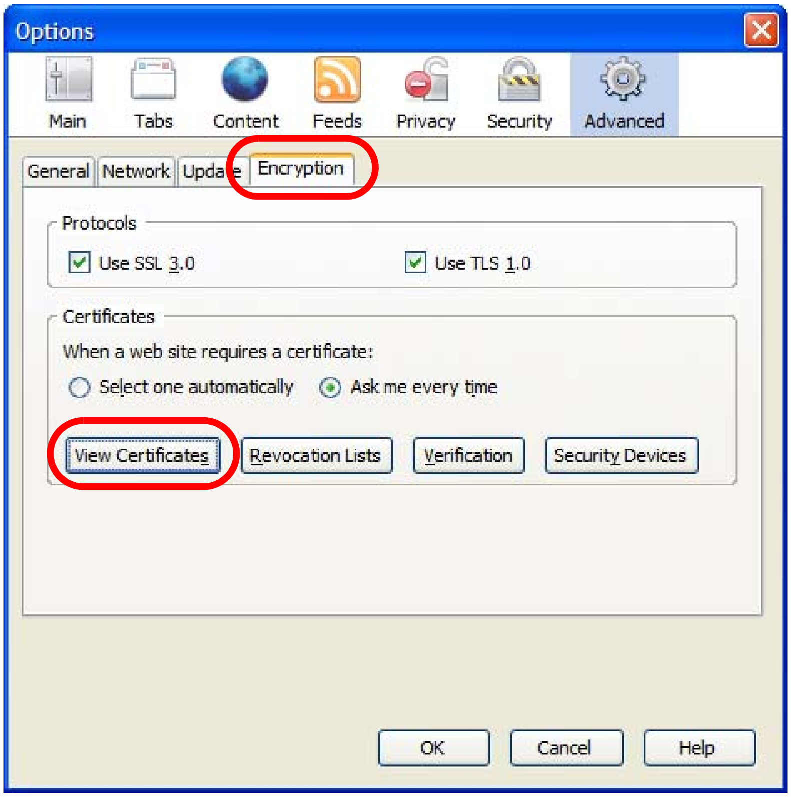
1 Open **Firefox** and click **Tools** > **Options**.

Figure 555 Firefox 2: Tools Menu


Tools
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Java Console
Error Console
Page Info
Clear Private Data... Ctrl+Shift+Del
Options...

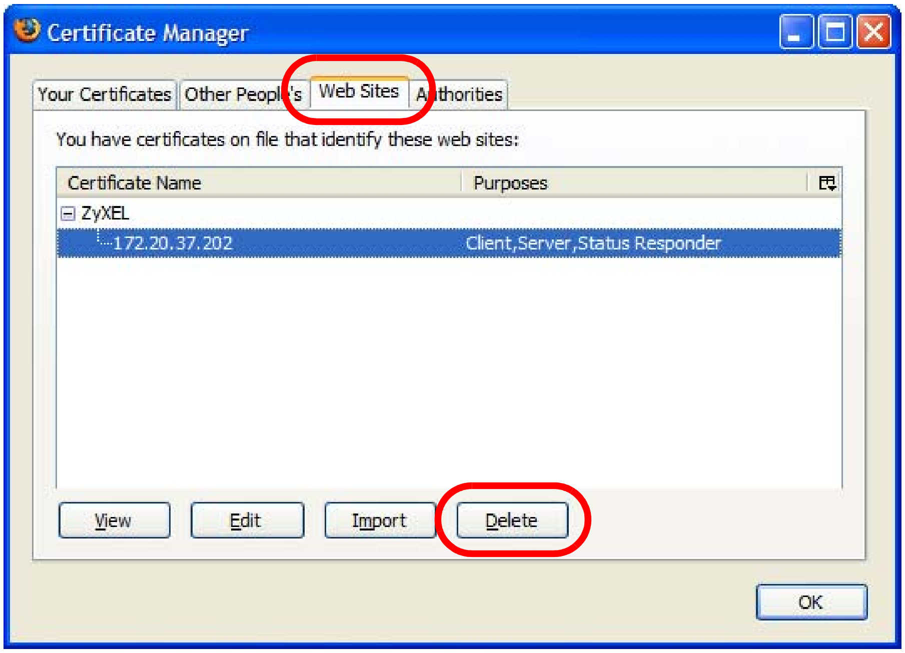
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 556 Firefox 2: Options


Options
Main
Tabs
Content
Feeds
Privacy
Security
Advanced
General
Network
Update
Encryption
Protocols
Use SSL 3.0
Use TLS 1.0
Certificates
When a web site requires a certificate:
Select one automatically
Ask me every time
View Certificates
Revocation Lists
Verification
Security Devices
OK
Cancel
Help

3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 557 Firefox 2: Certificate Manager

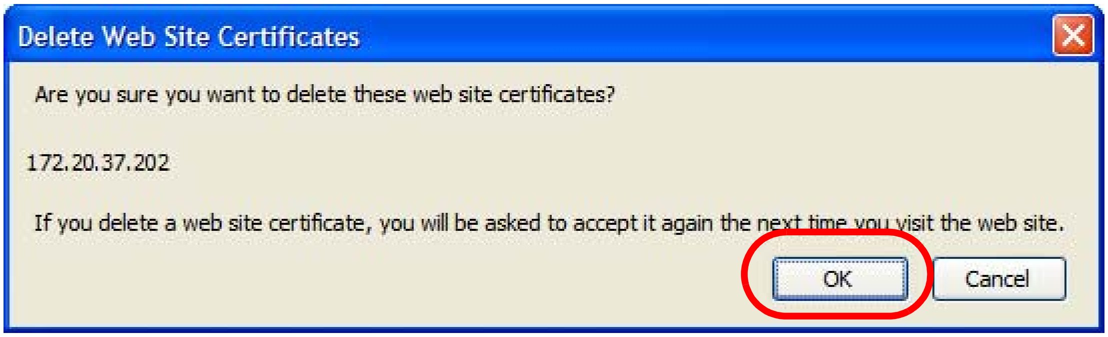

Certificate Manager
Your Certificates
Other Peopl 's
Web Sites
A thorities
View
Edit
Import
Delete
OK

You have certificates on file that identify these web sites:

Certificate Name	Purposes
ZyXEL	
172.20.37.202	Client,Server,Status Responder

4 In the **Delete Web Site Certificates** dialog box, click **OK**.

Figure 558 Firefox 2: Delete Web Site Certificates


Delete Web Site Certificates
OK
Cancel

Are you sure you want to delete these web site certificates?

172.20.37.202

If you delete a web site certificate, you will be asked to accept it again the next time you visit the web site.

5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

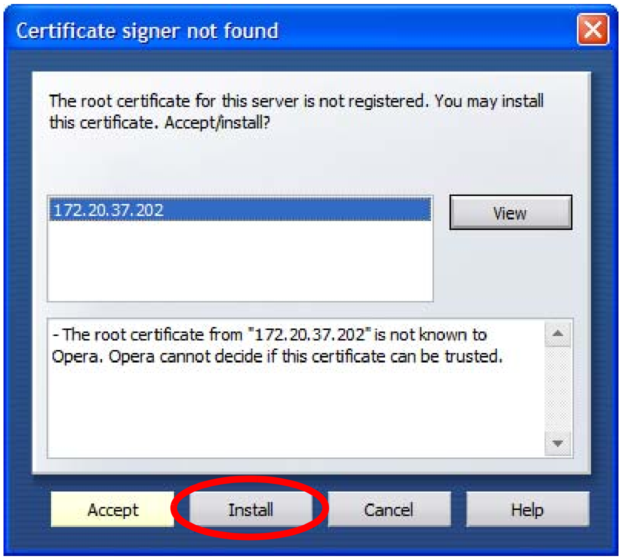
Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

1 If your device’s Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

2 Click **Install** to accept the certificate.

Figure 559 Opera 9: Certificate signer not found



Certificate signer not found

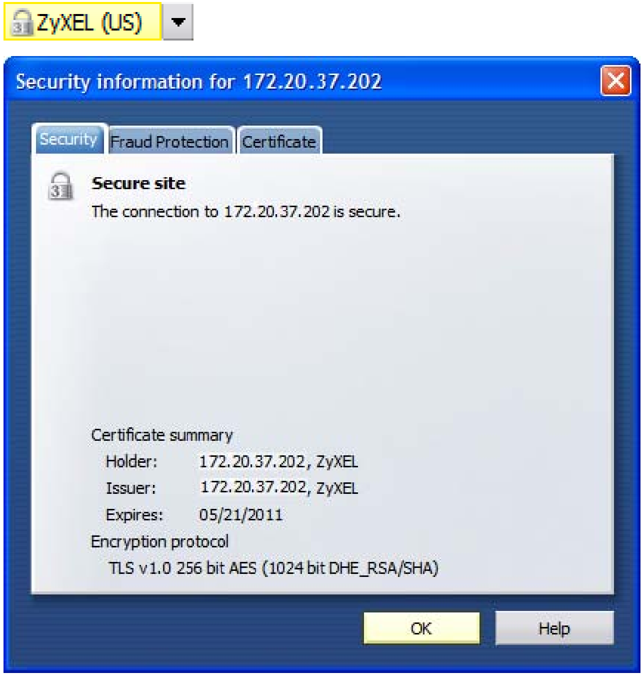
The root certificate for this server is not registered. You may install this certificate. Accept/install?

172.20.37.202

- The root certificate from "172.20.37.202" is not known to Opera. Opera cannot decide if this certificate can be trusted.

3 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Figure 560 Opera 9: Security information



Security information for 172.20.37.202

Secure site

The connection to 172.20.37.202 is secure.

Certificate summary

Holder: 172.20.37.202, ZyXEL

Issuer: 172.20.37.202, ZyXEL

Expires: 05/21/2011

Encryption protocol

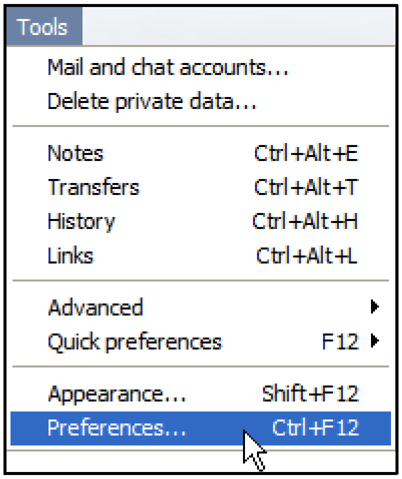
TLS v1.0 256 bit AES (1024 bit DHE_RSA/SHA)

Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

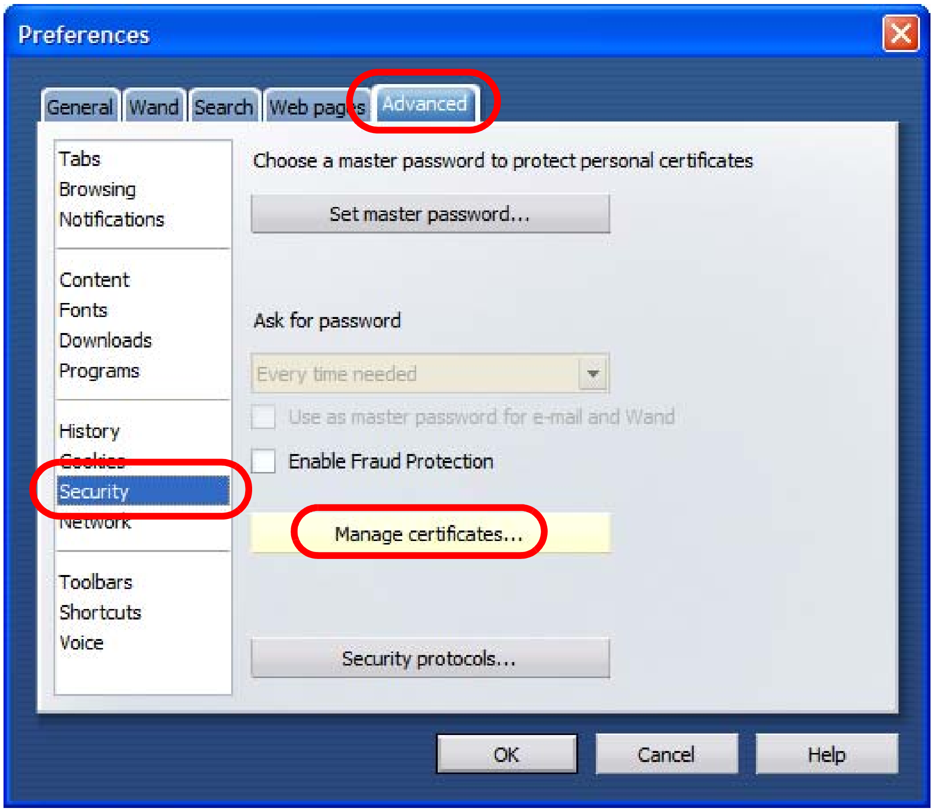
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 561 Opera 9: Tools Menu


Tools
Mail and chat accounts...
Delete private data...
Notes Ctrl+Alt+E
Transfers Ctrl+Alt+T
History Ctrl+Alt+H
Links Ctrl+Alt+L
Advanced
Quick preferences F12
Appearance... Shift+F12
Preferences... Ctrl+F12

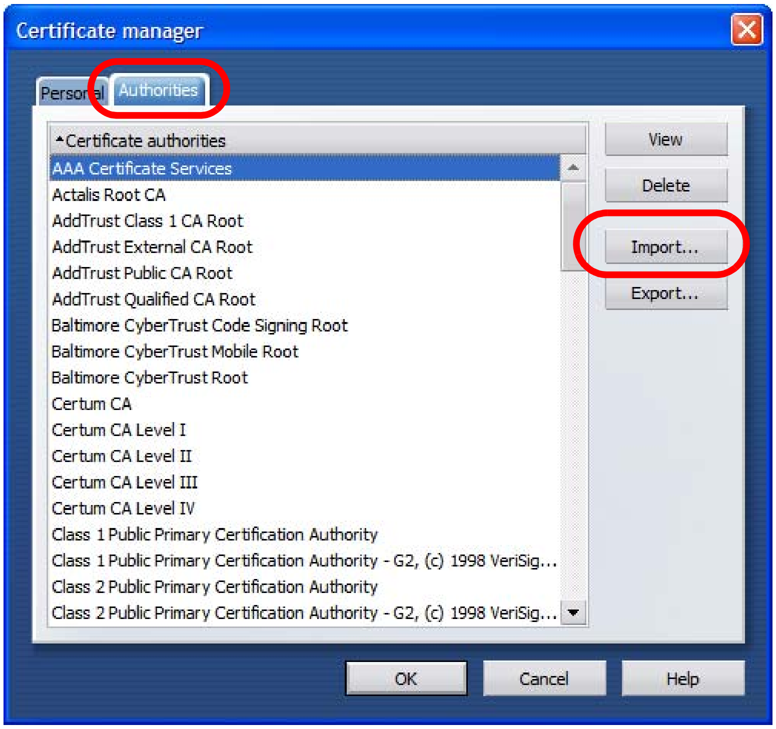
2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

Figure 562 Opera 9: Preferences


Preferences
General
Wand
Search
Web pages
Advanced
Tabs
Browsing
Notifications
Content
Fonts
Downloads
Programs
History
Cookies
Security
Network
Toolbars
Shortcuts
Voice
Choose a master password to protect personal certificates
Set master password...
Ask for password
Every time needed
☐ Use as master password for e-mail and Wand
☐ Enable Fraud Protection
Manage certificates...
Security protocols...
OK
Cancel
Help

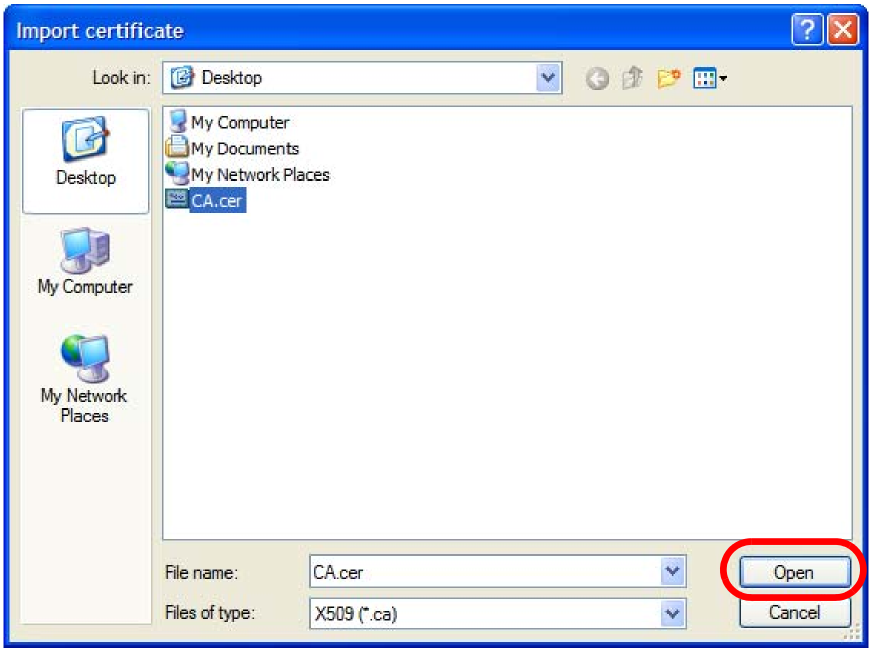
3 In the **Certificates Manager**, click **Authorities** > **Import**.

Figure 563 Opera 9: Certificate manager


Certificate manager
Personal
Authorities
Certificate authorities
AAA Certificate Services
Actalis Root CA
AddTrust Class 1 CA Root
AddTrust External CA Root
AddTrust Public CA Root
AddTrust Qualified CA Root
Baltimore CyberTrust Code Signing Root
Baltimore CyberTrust Mobile Root
Baltimore CyberTrust Root
Certum CA
Certum CA Level I
Certum CA Level II
Certum CA Level III
Certum CA Level IV
Class 1 Public Primary Certification Authority
Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSig...
Class 2 Public Primary Certification Authority
Class 2 Public Primary Certification Authority - G2, (c) 1998 VeriSig...
View
Delete
Import...
Export...
OK
Cancel
Help

4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

Figure 564 Opera 9: Import certificate

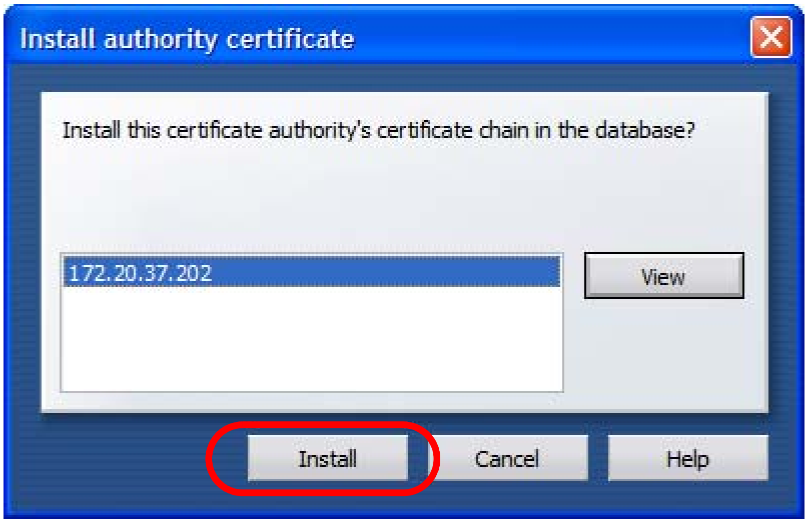

Import certificate
Look in:
Desktop
My Computer
My Documents
My Network Places
CA.cer
Desktop
My Computer
My Network Places
Open
Cancel

File name: CA.cer

Files of type: X509 (*.ca)

5 In the **Install authority certificate** dialog box, click **Install**.

Figure 565 Opera 9: Install authority certificate



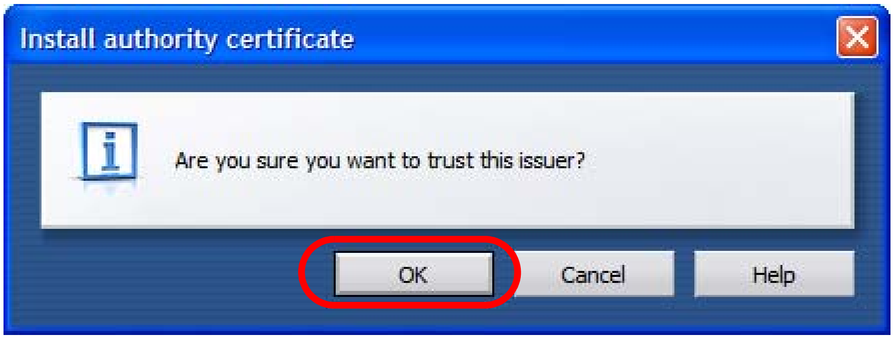
Install authority certificate

Install this certificate authority's certificate chain in the database?

172.20.37.202

6 Next, click **OK**.

Figure 566 Opera 9: Install authority certificate



Install authority certificate

Are you sure you want to trust this issuer?

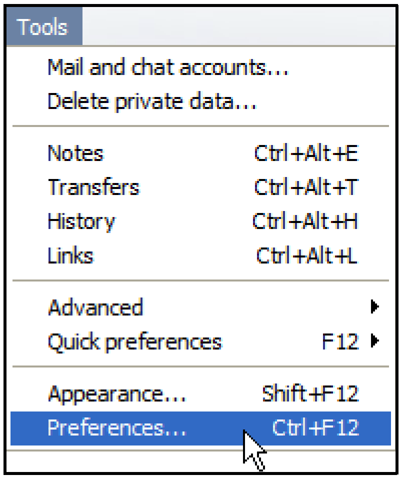
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

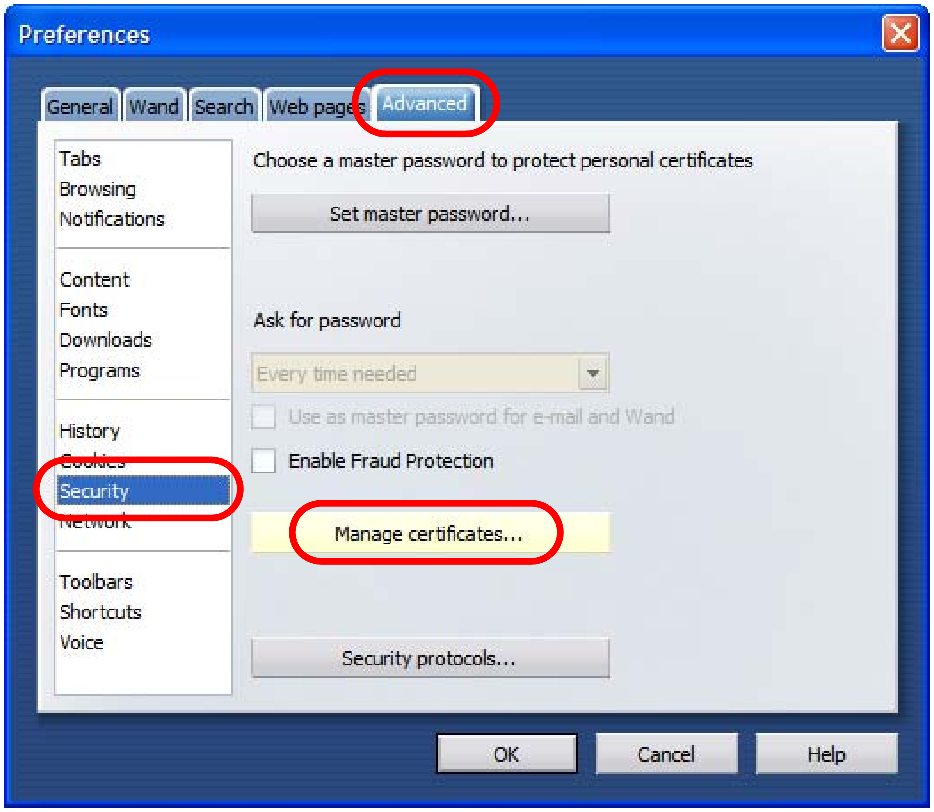
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 567 Opera 9: Tools Menu


Tools
Mail and chat accounts...
Delete private data...
Notes Ctrl+Alt+E
Transfers Ctrl+Alt+T
History Ctrl+Alt+H
Links Ctrl+Alt+L
Advanced
Quick preferences F12
Appearance... Shift+F12
Preferences... Ctrl+F12

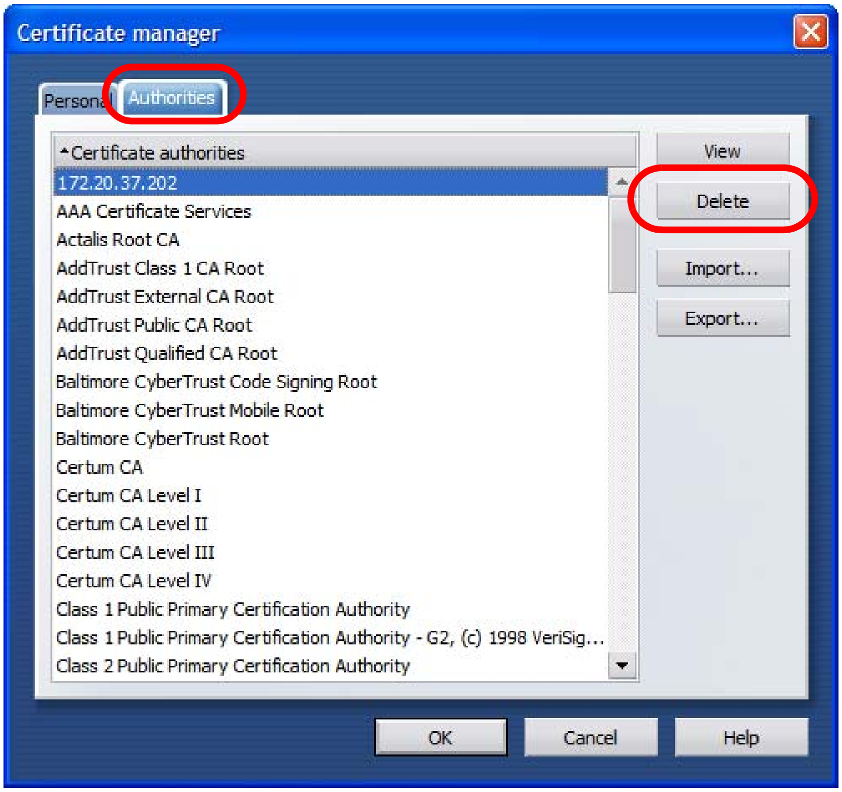
2 In **Preferences**, **Advanced** > **Security** > **Manage certificates**.

Figure 568 Opera 9: Preferences


Preferences
General
Wand
Search
Web pages
Advanced
Tabs
Browsing
Notifications
Content
Fonts
Downloads
Programs
History
Cookies
Security
Network
Toolbars
Shortcuts
Voice
Choose a master password to protect personal certificates
Set master password...
Ask for password
Every time needed
☐ Use as master password for e-mail and Wand
☐ Enable Fraud Protection
Manage certificates...
Security protocols...
OK
Cancel
Help

3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 569 Opera 9: Certificate manager


Certificate manager
Personal
Authorities
Certificate authorities
172.20.37.202
AAA Certificate Services
Actalis Root CA
AddTrust Class 1 CA Root
AddTrust External CA Root
AddTrust Public CA Root
AddTrust Qualified CA Root
Baltimore CyberTrust Code Signing Root
Baltimore CyberTrust Mobile Root
Baltimore CyberTrust Root
Certum CA
Certum CA Level I
Certum CA Level II
Certum CA Level III
Certum CA Level IV
Class 1 Public Primary Certification Authority
Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSig...
Class 2 Public Primary Certification Authority
View
Delete
Import...
Export...
OK
Cancel
Help

4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

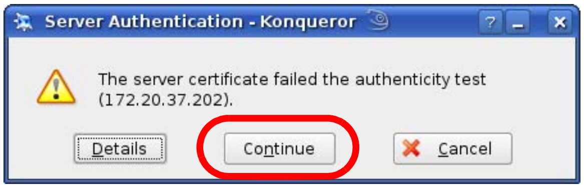
Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

1 If your device’s Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

2 Click **Continue**.

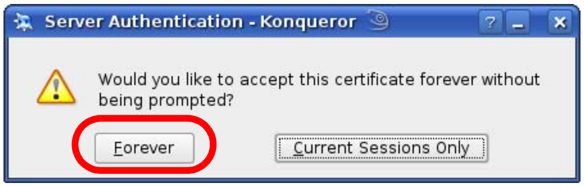
Figure 570 Konqueror 3.5: Server Authentication


Server Authentication - Konqueror
Details
Continue
Cancel

The server certificate failed the authenticity test (172.20.37.202).

3 Click **Forever** when prompted to accept the certificate.

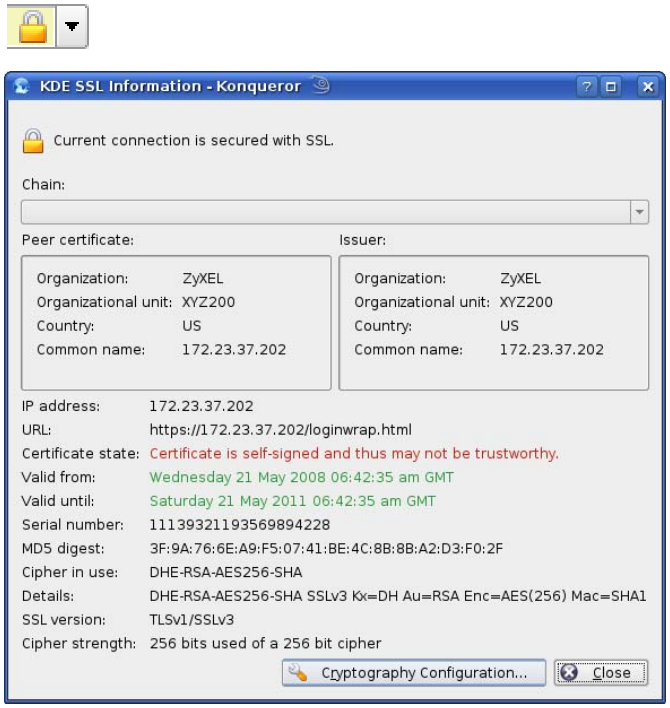
Figure 571 Konqueror 3.5: Server Authentication



Would you like to accept this certificate forever without being prompted?

4 Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

Figure 572 Konqueror 3.5: KDE SSL Information



KDE SSL Information - Konqueror
Cryptography Configuration...
Close

Current connection is secured with SSL.

Chain:

Peer certificate:
Organization: ZyXEL
Organizational unit: XYZ200
Country: US
Common name: 172.23.37.202

Issuer:
Organization: ZyXEL
Organizational unit: XYZ200
Country: US
Common name: 172.23.37.202

IP address: 172.23.37.202
URL: https://172.23.37.202/loginwrap.html
Certificate state: Certificate is self-signed and thus may not be trustworthy.
Valid from: Wednesday 21 May 2008 06:42:35 am GMT
Valid until: Saturday 21 May 2011 06:42:35 am GMT
Serial number: 11139321193569894228
MD5 digest: 3F:9A:76:6E:A9:F5:07:41:BE:4C:8B:8B:A2:D3:F0:2F
Cipher in use: DHE-RSA-AES256-SHA
Details: DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
SSL version: TLSv1/SSLv3
Cipher strength: 256 bits used of a 256 bit cipher

Installing a Stand-Alone Certificate File in Konqueror

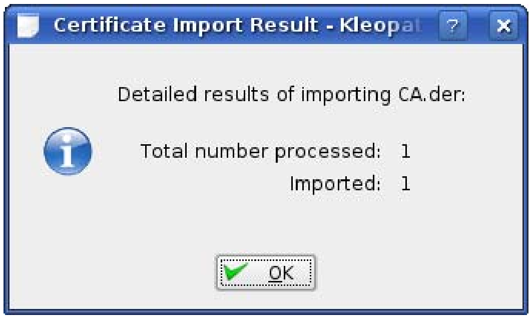
Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 573 Konqueror 3.5: Public Key Certificate File

2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

Figure 574 Konqueror 3.5: Certificate Import Result



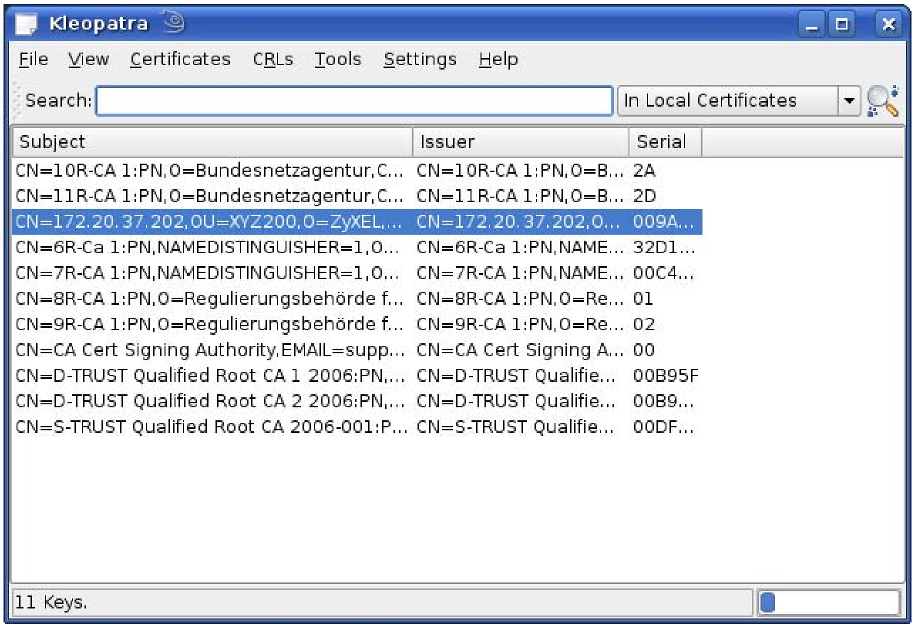
Detailed results of importing CA.der:

Total number processed: 1

Imported: 1

The public key certificate appears in the KDE certificate manager, **Kleopatra**.

Figure 575 Konqueror 3.5: Kleopatra



Subject	Issuer	Serial
CN=10R-CA 1:PN,O=Bundesnetzagentur,C...	CN=10R-CA 1:PN,O=B...	2A
CN=11R-CA 1:PN,O=Bundesnetzagentur,C...	CN=11R-CA 1:PN,O=B...	2D
CN=172.20.37.202,OU=XYZ200,O=ZyXEL,...	CN=172.20.37.202,O...	009A...
CN=6R-Ca 1:PN,NAMEDISTINGUISHER=1,O...	CN=6R-Ca 1:PN,NAME...	32D1...
CN=7R-CA 1:PN,NAMEDISTINGUISHER=1,O...	CN=7R-CA 1:PN,NAME...	00C4...
CN=8R-CA 1:PN,O=Regulierungsbehörde f...	CN=8R-CA 1:PN,O=Re...	01
CN=9R-CA 1:PN,O=Regulierungsbehörde f...	CN=9R-CA 1:PN,O=Re...	02
CN=CA Cert Signing Authority,EMAIL=supp...	CN=CA Cert Signing A...	00
CN=D-TRUST Qualified Root CA 1 2006:PN,...	CN=D-TRUST Qualifie...	00B95F
CN=D-TRUST Qualified Root CA 2 2006:PN,...	CN=D-TRUST Qualifie...	00B9...
CN=S-TRUST Qualified Root CA 2006-001:P...	CN=S-TRUST Qualifie...	00DF...

11 Keys.

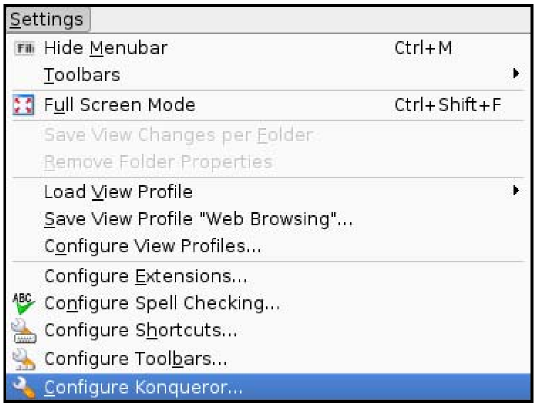
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open **Konqueror** and click **Settings > Configure Konqueror**.

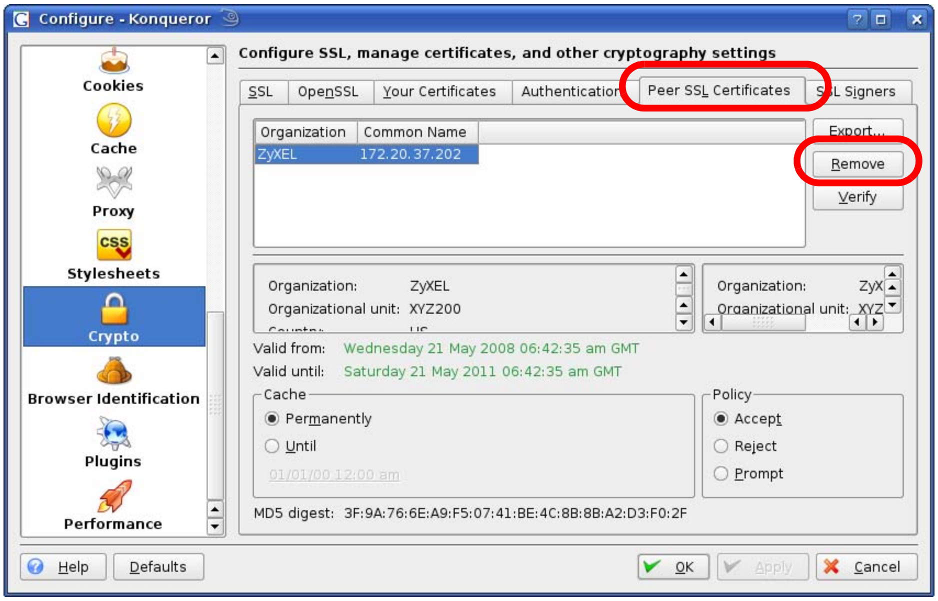
Figure 576 Konqueror 3.5: Settings Menu


Settings
Hide Menubar Ctrl+M
Toolbars
Full Screen Mode Ctrl+Shift+F
Save View Changes per Folder
Remove Folder Properties
Load View Profile
Save View Profile "Web Browsing"...
Configure View Profiles...
Configure Extensions...
Configure Spell Checking...
Configure Shortcuts...
Configure Toolbars...
Configure Konqueror...

2 In the **Configure** dialog box, select **Crypto**.

3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

Figure 577 Konqueror 3.5: Configure


Configure - Konqueror
Cookies
Cache
Proxy
Stylesheets
Crypto
Browser Identification
Plugins
Performance
SSL
OpenSSL
Your Certificates
Authentication
Peer SSL Certificates
SSL Signers
Export...
Remove
Verify
Help
Defaults
OK
Apply
Cancel

Configure SSL, manage certificates, and other cryptography settings

Organization	Common Name
ZyXEL	172.20.37.202

Organization: ZyXEL
Organizational unit: XYZ200

Organization: ZyX
Organizational unit: XYZ

Valid from: Wednesday 21 May 2008 06:42:35 am GMT
Valid until: Saturday 21 May 2011 06:42:35 am GMT

Cache
● Permanently
○ Until
01/01/00 12:00 am

Policy
● Accept
○ Reject
○ Prompt

MD5 digest: 3F:9A:76:6E:A9:F5:07:41:BE:4C:8B:8B:A2:D3:F0:2F

4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

D

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the ISG50 is subject to the terms and conditions of any related service providers.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

Go to http://www.zyxel.com to view this product’s documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

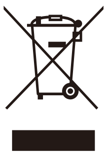
Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Index

Symbols

Numbers

3322 Dynamic DNS 317

3DES 387

3G 109

3G see also cellular 251

A

AA 479, 497, 500

AAA
  Base DN 633
  Bind DN 634, 636
  directory structure 633
  Distinguished Name, see DN
  DN 633, 634, 635, 636
  password 636
  port 635, 638
  search time limit 636

AAA server 631
  AD 633
  and users 600
  directory service 631
  LDAP 631, 633
  local user database 632
  object, where used 103
  RADIUS 631, 633, 636
  RADIUS group 637
  see also RADIUS

AbS 475

access 43

Access Point Name, see APN

access users 599, 601
  custom page 683
  forcing login 347
  idle timeout 607
  logging in 347
  multiple logins 608
  see also users 599
  Web Configurator 609

access users, see also force user authentication policies

account
  myZyXEL.com 230, 231
  user 599

accounting server 631

ACD queue 219

Active Directory, see AD

active protocol 392
  AH 392
  and encapsulation 392
  ESP 392

active sessions 189, 191, 203

AD 631, 633, 634, 635, 636
  directory structure 633
  Distinguished Name, see DN
  password 636
  port 635, 638
  search time limit 636

adapter, telephone
  see ATA

Adaptive Differential Pulse Code Modulation
  see ADPCM

address book 587

address groups 613
  and firewall 351, 363
  and FTP 700
  and SNMP 703
  and SSH 696
  and Telnet 699
  and WWW 683
  where used 103

address objects 613
  and firewall 351, 363
  and FTP 700
  and NAT 296, 326
  and policy routes 295

- and SNMP 703
- and SSH 696
- and Telnet 699
- and VPN connections 370
- and WWW 683
- HOST 613
- RANGE 613
- SUBNET 613
- types of 613
- where used 103

address record 674

admin user
- troubleshooting 771

admin users 599
- multiple logins 607
- see also users 599

ADP 411
- base profiles 412, 414
- configuration overview 103
- false negatives 415
- false positives 415
- inline profile 415
- monitor profile 415
- port scanning 421
- prerequisites 102, 103
- protocol anomaly 411
- traffic anomaly 411, 415

ADPCM 475

Advanced Encryption Standard, see AES

AES 387

AF 299

after hours 466, 763

aged file 720

AH 374, 392
- and transport mode 392

a-law 470

alerts 707, 711, 712, 713, 716, 717, 718

ALG 335, 339
- and firewall 335, 336
- and NAT 335, 336
- and policy routes 336, 339
- and trunks 339
- configuration overview 101
- FTP 335
- H.323 335, 339
- peer-to-peer calls 336
- RTP 340
- see also VoIP pass through 335
- SIP 335, 336
- tutorial 125

AMR-WB 470

analog
- audio 475
- extension settings 449
- FXO line settings 450
- telephones 88

Analog Telephone Adapter
- see ATA

Analysis-by-Synthesis
- see AbS

Anomaly Detection and Prevention, see ADP

Apache server 425, 426

Apache-whitespace attack 425

APN 255

Application Layer Gateway, see ALG

application order 94

applications, critical 430

ASAS (Authenex Strong Authentication System) 632

ASCII-encoding 425

ASCII-encoding attacks 425

assured forwarding 447

asymmetrical routes 360
- allowing through the firewall 361
- vs virtual interfaces 360

ATA 37

attacks
- Apache-whitespace 425
- ASCII-encoding 425
- bare byte encoding 425
- base36-encoding 425
- Denial of Service (DoS) 373
- directory traversal 425
- double-encoding 425
- IIS-backslash-evasion 425
- IIS-unicode-codepoint-encoding 425
- multi-slash-encoding 425
- network-based 42
- non-RFC-defined-char 425
- non-RFC-HTTP-delimiter 425
- obsolete-options 426
- oversize-chunk-encoding 425
- oversize-len 426
- oversize-offset 426
- oversize-request-uri-directory 426

    - self-directory-traversal attack 426
    - truncated-address-header 427
    - truncated-header 426, 427
    - truncated-options 426
    - truncated-timestamp-header 427
    - TTCP-detected 426
    - u-encoding 426
    - undersize-len 426
    - undersize-offset 426
    - UTF-8-encoding 426
- audio
  - files 532, 533
    - for auto-attendant 510
    - recording 516
  - on hold 539
  - sampling 475
- audio files
  - format 510
- Authenex Strong Authentication System (ASAS) 632
- authentication
  - in IPSec 375
  - LDAP/AD 633
  - server 631
- authentication algorithms 312, 387
  - and active protocol 387
  - and routing protocols 312
  - MD5 312, 387
  - SHA1 387
  - text 312
- Authentication Header, see AH
- authentication method objects 639
  - and users 600
  - and WWW 682
  - create 641
  - example 639
  - where used 103
- authentication policy 347
  - exceptional services 349
- authentication type 73, 663
- Authentication, Authorization, Accounting servers, see AAA server
- authority groups 88
  - add 458
  - and call access code 453
  - and call routing 89
  - and extensions 88
  - configuration 459
  - creation guidelines 455
  - creation tutorial 137
  - descriptions 458
  - edit 458
  - extensions 455
  - features 462
    - call blocking 462
    - call forwarding 462
  - group names 458
  - grouping 455
  - LCRs 146, 152, 158, 527
  - limitations 455
  - management 527
- authorization server 631
- Auto Attendant
  - see AA
- auto callback 532, 533
- auto configuration 141
- auto provisioning 141
  - client configuration 142
  - MAC address 142
  - overview 573
  - serial number 142
  - settings 577
- auto-attendant 89, 151, 503, 595
  - adding, deleting 508
  - advanced example 504
  - and fax 89, 503
  - audio
    - files 510
  - BRI trunk 502
  - call routing 503
  - diagram 504
  - FXO trunks 496
  - management 507
  - menus 504
  - night service 513
  - recording instructions 516
  - SIP trunks 486, 493
  - structure 504
- automatic switchboard operator 503

B

- backing up configuration files 727
- backslashes 425

bad-length-options attack 426
bandwidth 430
  egress 256
  ingress 256
bandwidth limit
  troubleshooting 768
bandwidth management
  and policy routes 297
  interface, outbound, see interfaces
  maximize bandwidth usage 297, 300, 400, 401
  see also policy routes
bare byte encoding 425
bare byte encoding attack 425
Base DN 633
base profiles
  in ADP 412, 414
base36-encoding 425
base36-encoding attack 425
basic PBX setup tutorial 135
Basic Rate Interface
  see BRI
Bind DN 634, 636
black list 466, 761, 763
blind forward 465, 762
blocking calls 462, 463, 761
boot module 732
BRI 447, 448
  PBX 478
  settings 451
  switch types 449
  trunk 478
    adding and editing 502
    auto-attendant 502
    settings 497
BRI trunk monitor 218
bridge interfaces 234, 268
  and virtual interfaces of members 269
  basic characteristics 234
  effect on routing table 269
  member interfaces 268
bridges 268
busy forward 465, 762

C

CA
  and certificates 644
CA (Certificate Authority), see certificates
call access code 453
call blocking 462, 463, 466
  settings 542
Call Detail Record
  see CDR
call features 163, 532
call forwarding 433, 462, 463, 761
call handling 595
call length, maximum 581
call parking 532, 534
  configuration 535
  overview 534, 536
call recording 544, 764
call recordings 222
call records query 225, 227
call restrictions 455
call routing terms 87
call services 532
  auto callback 533
  call parking 534
  call transfer 541
  call waiting 536
  conference calls 547
  emergency call 538
  MOH 539
call transfer 433, 532, 541
  configuration 542
call waiting 532, 536
  configuration 537
callback, auto 532, 533
caller ID 466
calling emergency numbers 538
calls
  between extensions 89
  emergency 532
  to ITSP 88
  to PSTN 88
calls, emergency 532, 533
capturing packets 739
card SIM 256

CDR 720
  aged file 720
  backup results 223
  executing SQL script 721
  external server 721
  local database 720
  management 721
  overview 720
  PostgreSQL 721
  query 225, 227
  remote server configuring procedure 722
  types of files 720
CEF (Common Event Format) 709, 716
cellular 109, 251
  APN 255
  band selection 257
  interfaces 234
  signal quality 208, 209
  SIM card 256
  status 210
  system 208, 209
  troubleshooting 767
certificate
  troubleshooting 771
Certificate Authority (CA)
  see certificates
Certificate Management Protocol (CMP) 650
Certificate Revocation List (CRL) 644
  vs OCSP 659
certificates 643
  advantages of 644
  and CA 644
  and FTP 700
  and HTTPS 679
  and IKE SA 391
  and SSH 696
  and VPN gateways 370
  and WWW 681
  certification path 644, 652, 657
  expired 644
  factory-default 644
  file formats 644
  fingerprints 653, 658
  importing 647
  in IPSec 382
  not used for encryption 644
  revoked 644
  self-signed 644, 649
  serial number 652, 657
  storage space 647, 655
  thumbprint algorithms 646
  thumbprints 646
  used for authentication 644
  verifying fingerprints 645
  where used 103
certification requests 649, 650
certifications 855
  notices 855
  viewing 855
Challenge Handshake Authentication Protocol (CHAP) 663
CHAP (Challenge Handshake Authentication Protocol) 663
CHAP/PAP 663
checking order 94
circuit-switched 447
class selector 447
CLI 35, 54
  button 54
  messages 54
  popup window 54
  Reference Guide 2
codecs 468, 475
  SIP trunk 486, 493
coder/decoders 470, 475
cold start 36
commands 35
  sent by Web Configurator 54
Common Event Format (CEF) 709, 716
common services 827
compression
  audio 475
  video 475
compression (stac) 663
computer names 244, 266, 273, 278
conference calls 532, 547
  add 547
  edit 547
  maximum number of members 548
  overview 547
conference room 548
conference, meet-me 532
configuration
  information 737, 742
  object-based 91
  overview 97

- text file 141
- configuration file
  - troubleshooting 773
- configuration files 725
  - at restart 728
  - backing up 727
  - downloading 729
  - downloading with FTP 699
  - editing 725
  - how applied 726
  - lastgood.conf 728, 731
  - managing 727
  - not stopping or starting the device 36
  - startup-config.conf 731
  - startup-config-bad.conf 728
  - syntax 726
  - system-default.conf 731
  - uploading 731
  - uploading with FTP 699
  - use without restart 725
- congestion 447
- connecting IP telephones 140
- connecting to ITSP 148
- connecting to PSTN 143
- connection
  - troubleshooting 769
- connectivity check 243, 251, 256, 265, 274, 375
- console port 35
  - speed 671
- cookies 43
- copyright 855
- CoS 447
- country code 450
- CPU usage 189, 190
- critical applications 430
- CTI peer monitor 216
- current date/time 188, 667
  - and schedules 625
  - daylight savings 669
  - setting manually 670
  - time server 671
- custom
  - access user page 683
  - login page 683

D

- Data Encryption Standard, see DES
- Database Management System
  - see DBMS
- date 667
- daylight savings 669
- daytime call handling 595
- DBMS 720
- DDI 500
- DDNS 317
  - backup mail exchanger 321
  - configuration overview 100
  - mail exchanger 321
  - prerequisites 100
  - service providers 317
  - troubleshooting 768
- Dead Peer Detection, see DPD
- decoders 468, 470
- default
  - firewall behavior 354
  - interfaces and zones 93
- delay 430
- Delta PCM 475
- Denial of Service (Dos) attacks 373
- deployment
  - and auto provisioning 141
- DES 387
- device access
  - troubleshooting 765
- device introduction 28
- DHCP 277, 666
  - and DNS servers 278
  - and domain name 666
  - and interfaces 278
  - client list 192
  - pool 278
  - static DHCP 278
- diagnostics 737, 742
- dial condition 88
  - examples 145, 152, 157
- dialing rules 151
- DID 500
- Differential PCM 475
- Diffie-Hellman key group 388

DiffServ 299, 430, 447
DiffServ Code Point
  see DSCP
digit handling 451
digital sampling 475
Digital Signature Algorithm public-key algorithm, see DSA
direct pickup 433
direct routes 292
directory 631
directory service 631
  file structure 633
directory traversal attack 425
directory traversals 425
disclaimer 855
Distinguished Name (DN) 633, 634, 635, 636
distributed port scans 422
DN 633, 634, 635, 636
DND 433, 462, 465, 762
DNS 672
  address records 674
  domain name forwarders 675
  domain name to IP address 674
  IP address to domain name 675
  Mail eXchange (MX) records 676
  pointer (PTR) records 675
DNS servers 74, 672, 675
  and interfaces 278
documentation
  related 2
domain name 666
Domain Name System, see DNS
double-encoding attack 425
DPD 385
drop precedence 447
DSA 649
DSCP 293, 295, 430, 447, 749
DSP 38
  resources 547
DTMF 468, 469, 470, 484, 491
Dynamic Domain Name System, see DDNS
Dynamic Host Configuration Protocol, see DHCP.
dynamic peers in IPSec 373
DynDNS 317
DynDNS see also DDNS 317
Dynu 317

E

E911 532
echo 430
EGP (Exterior Gateway Protocol) 421
egress bandwidth 256
e-mail
  daily statistics report 706
email, attaching voice file 764
emergency calls 532, 533
  configuration 538
  overview 532
en-bloc 451
Encapsulating Security Payload, see ESP
encapsulation
  and active protocol 392
  IPSec 374
  transport mode 392
  tunnel mode 392
  VPN 392
encryption
  IPSec 374
  RSA 652
encryption algorithms 387
  3DES 387
  AES 387
  and active protocol 387
  DES 387
encryption method 663
enforcing policies in IPSec 374
Enhanced 911
  see E911
ESP 374, 392
  and transport mode 392
Ethernet interfaces 107, 234
  and OSPF 239
  and RIP 238
  and routing protocols 237
  basic characteristics 234
examples (tutorials) 107
exceptional services 349
expedited forwarding 447
experimental-options attack 426

export phonebook 588

extended authentication
  and VPN gateways 370
  IKE SA 391

extension portal 757
  account settings 760
  call forward and blocking 761
  call recording 764
  restrictions 760
  voice mail 763
  web phone dial 759

extensions 27, 87, 89, 136
  busy 532
  call transfer 532
  for analog phones 88
  FXS 88
  grouping 455
  ISDN BRI 88
  portal 757
  query number 458
  ring groups 549
  SIP 87
  user login 757
  voice mail 467

external lines
  see outbound line groups

ext-user
  troubleshooting 771

F

false negatives 415

false positives 415, 417

fax 89, 503

FCC interference statement 855

feature code
  settings 433

feature codes 163
  example 163
  tutorial 163
  voice mail 163

file extensions
  configuration files 725
  shell scripts 725

file manager 725
  configuration overview 105

filtered port scan 422

find me list 761

Firefox 43

firewall 353, 354
  actions 364
  and address groups 351, 363
  and address objects 351, 363
  and ALG 335, 336
  and H.323 (ALG) 335
  and HTTP redirect 332
  and IPSec SA 355
  and IPSec VPN 770
  and logs 351, 364
  and NAT 361
  and port triggering 296, 768
  and schedules 351, 363, 405, 407
  and service groups 363
  and service objects 620
  and services 363
  and user groups 363, 366
  and users 363, 366
  and VoIP pass through 336
  and zones 354, 362
  asymmetrical routes 360, 361
  configuration overview 101
  global rules 355
  prerequisites 102
  priority 362
  rule criteria 355
  see also to-Device firewall 354
  session limits 355, 364
  to-Device, see to-Device firewall
  triangle routes 360, 361
  troubleshooting 766

firmware
  and restart 731
  boot module, see boot module
  current version 187, 732
  getting updated 731
  uploading 731, 732
  uploading with FTP 699

firmware upload
  troubleshooting 773

flash usage 189

flood detection 423

follow me 433

force user authentication policies
  prerequisites 104

forcing login 347

Foreign Exchange Office
  see FXO

Foreign Exchange Subscriber
  see FXS

forwarding calls 463

FQDN 674

fragmenting IPSec packets 371

FTP 699
  additional signaling port 339
  ALG 335
  and address groups 700
  and address objects 700
  and certificates 700
  and zones 700
  signaling port 338
  with Transport Layer Security (TLS) 700

Fully-Qualified Domain Name, see FQDN

functional overview 87

FXO 448
  and FXS relationship 88
  ports 88, 143
  settings 450
  trunk 88, 144, 156, 478
    adding and editing 495

FXO trunk
  auto-attendant 496

FXO trunk monitor 217

FXS 448
  and FXO relationship 88
  extensions 88
  ports 88

FXS settings 449

G

G.279 475

G.711 470, 475

G.722 470, 475

G.723.1 475

G.726 470, 475

G.729 470

G.729A 470

gateway policy, see VPN gateways

Generic Routing Encapsulation, see GRE.

global PBX settings 429

GRE 279

group management 526
  associate to authority and outbound line groups 530
  granting calling rights 526

group pickup 433, 468, 469

groups, ring 549

GSM 256

Guide
  CLI Reference 2
  Quick Start 2

H

H.261 470, 476

H.263 470, 476

H.264 476
  MP4 470

H.323 125, 339
  additional signaling port 338
  ALG 335, 339
  and firewall 335
  and RTP 340
  signaling port 338

hold 532, 533

hop 447

hours 595

HSDPA 256

HTML-based phone 757, 759

HTTP 574
  inspection 418, 425
  over SSL, see HTTPS
  redirect to HTTPS 681
  vs HTTPS 679

HTTP redirect 331
  and firewall 332
  and interfaces 334
  and policy routes 332
  configuration overview 101
  packet flow 332
  prerequisites 101
  troubleshooting 769

HTTPS 123, 679
  and certificates 679

  authenticating clients 679
  avoiding warning messages 687
  example 687
  vs HTTP 679
  with Internet Explorer 687
hunt group 562
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

ICMP 619
  datagram length 427
  decoder 418, 425
  echo 423
  flood attack 423
  portsweep 422
  Time Stamp header length 427
  unreachables 422
IEEE 802.1q VLAN
IGP (Interior Gateway Protocol) 421
IIS
  backslash-evasion attack 425
  emulation 425
  encoding 425
  server 425
  unicode 425
  unicode-codepoint-encoding attack 425
IKE SA
  aggressive mode 386, 389, 390
  and certificates 391
  and RADIUS 391
  and to-Device firewall 770
  authentication algorithms 387
  content 389
  Dead Peer Detection (DPD) 385
  Diffie-Hellman key group 388
  encryption algorithms 387
  extended authentication 391
  ID type 389
  IP address, remote IPSec router 386
  IP address, ZyXEL device 386
  local identity 389
  main mode 386, 389, 390
  NAT traversal 390
  negotiation mode 386
  password 391
  peer identity 389
  pre-shared key 389
  proposal 387
  see also VPN
  user name 391
import phonebook 588
inbound calls, and auto-attendant 503, 504
incoming bandwidth 256
incoming calls
  handling 595
  second call 532
  transferring 532
ingress bandwidth 256
inline profile 415
Integrated Services Digital Network
  see ISDN
interconnected VoIP 532
interface
  status 188, 199
  troubleshooting 766
  types 92
interfaces 92, 107, 233
  and DNS servers 278
  and HTTP redirect 334
  and layer-3 virtualization 234
  and NAT 326
  and physical ports 92, 233
  and policy routes 296
  and static routes 298
  and VPN gateways 370
  and zones 92, 234
  as DHCP relays 278
  as DHCP servers 278, 666
  backup, see trunks
  bandwidth management 277, 288
  bridge, see also bridge interfaces.
  cellular 234
  configuration overview 98
  default configuration 93
  DHCP clients 276
  Ethernet, see also Ethernet interfaces.
  gateway 277
  general characteristics 233
  IP address 276
  metric 277
  MTU 277
  overlapping IP address and subnet mask 276
  port groups, see also port groups.

  PPPoE/PPTP, see also PPPoE/PPTP interfaces.
  prerequisites 98, 235
  relationships between 235
  static DHCP 278
  subnet mask 276
  trunks, see also trunks.
  types 234
  virtual, see also virtual interfaces.
  VLAN, see also VLAN interfaces.
  where used 98
internal calls 89
  routing 136
internal operator 433
internal telephone network 38
Internet access
  troubleshooting 766, 770
Internet Control Message Protocol, see ICMP
Internet Explorer 43
Internet Protocol Security, see IPSec
Internet Telephony Service Provider
  see ITSP
IP alias, see virtual interfaces
IP decoy portscan 422
IP distributed portscan 422
IP network 38
IP PBX 27
IP policy routing, see policy routes
IP portscan 421
IP portsweep 422
IP protocols 619
  and service objects 620
  ICMP, see ICMP
  TCP, see TCP
  UDP, see UDP
IP static routes, see static routes
IP telephone
  extensions 469
IP telephones 37, 136
  and auto provisioning 141
  deployment 140
  registration 140
IP/MAC binding 341
  exempt list 345
  monitor 205
  static DHCP 344
IPSec 367
  active protocol 374
  AH 374
  and certificates 370
  authentication 375
  basic troubleshooting 769
  certificates 382
  connections 370
  connectivity check 375
  encapsulation 374
  encryption 374
  ESP 374
  established in two phases 368
  fragmentation 371
  local network 367
  local policy 373
  manual key 373
  NetBIOS 373
  peer 367
  Perfect Forward Secrecy 375
  PFS 375
  phase 2 settings 374
  policy enforcement 374
  remote access 373
  remote IPSec router 367
  remote network 367
  remote policy 373
  replay detection 373
  SA life time 374
  SA monitor 211
  SA see also IPSec SA 391
  see also VPN
  site-to-site with dynamic peer 373
  static site-to-site 373
  transport encapsulation 374
  tunnel encapsulation 374
  VPN gateway 370
IPSec SA
  active protocol 392
  and firewall 355, 770
  and to-Device firewall 770
  authentication algorithms 387
  authentication key (manual keys) 393
  destination NAT for inbound traffic 395
  encapsulation 392
  encryption algorithms 387
  encryption key (manual keys) 393
  local policy 391
  manual keys 393
  NAT for inbound traffic 393
  NAT for outbound traffic 393

  Perfect Forward Secrecy (PFS) 392
  proposal 392
  remote policy 391
  search by name 212
  search by policy 212
  Security Parameter Index (SPI) (manual keys) 393
  see also IPSec
  see also VPN
  source NAT for inbound traffic 394
  source NAT for outbound traffic 394
  status 211
  transport mode 392
  tunnel mode 392
  when IKE SA is disconnected 391
IPSec VPN
  configuration overview 102
  prerequisites 101, 102
  see also IPSec
  troubleshooting 769
  tutorial 113
  where used 102
ISDN 447, 448
  B-channels 447
  BRI 447, 448
  BRI extensions 88
  calls tutorial 154
  D-channels 447
  network configuration, tutorial 159
  NT mode 448
  TE mode 448
ISP account
  CHAP 663
  CHAP/PAP 663
  MPPE 663
  MSCHAP 663
  MSCHAP-V2 663
  PAP 663
ISP accounts 661
  and PPPoE/PPTP interfaces 247, 661
  authentication type 663
  encryption method 663
  stac compression 663
ISUP 451
ITSP 27, 88, 478
ITSP calls, tutorial 147

J

Java
  permissions 43
JavaScripts 43
jitter buffer 430

K

key pairs 643

L

LAND attack 424
lastgood.conf 728, 731
latency 430
LCR 88, 89, 519
  adding or deleting a dial condition 523
  advanced setup 90
  and authority group 152, 158
  and authority groups 146
  and dialing conditions 88
  and outbound line groups 88
  associations 520
  associations example 519
  authority groups 527
  basic setup 90
  components 520
  components example 519
  configuration 521
  dial conditions 520
  example 90, 151, 152
  list 521
  outbound line groups 478, 520, 529
  tutorial 144, 156
LDAP 38, 587, 589, 631
  and users 600
  Base DN 633
  Bind DN 634, 636
  directory 631
  directory structure 633
  Distinguished Name, see DN
  DN 633, 634, 635, 636
  password 636
  port 635, 638

- search time limit 636
- user attributes 610

Least Cost Routing
- see LCR

least load first load balancing 283

LED troubleshooting 765

legacy PBX 28

license
- key 232
- upgrading 232

licensing 229

Lightweight Directory Access Protocol
- see LDAP

Lightweight Directory Access Protocol, see LDAP

listening volume 450

load balancing 281
- algorithms 282, 287
- least load first 283
- round robin 288
- see also trunks 281
- session-oriented 282
- spillover 284
- tutorial 111
- weighted round robin 283

local calls 88

local phonebook 587, 591, 592

local user database 632

log
- troubleshooting 772

log messages
- categories 712, 713, 716, 717, 718
- debugging 220
- regular 220
- types of 220

logged in users 193

login
- custom page 683

logo
- troubleshooting 772

logout
- Web Configurator 45

logs
- and firewall 351, 364
- configuration overview 105
- descriptions 775
- e-mail profiles 707
- e-mailing log messages 221, 711
- formats 709
- log consolidation 712
- settings 707
- syslog servers 707
- system 707
- types of 707

M

MAC address
- and VLAN 260
- Ethernet interface 242
- range 187

making internal calls, tutorial 136

management access
- troubleshooting 772

Management Information Base (MIB) 701, 702

managing authority groups 526, 527

managing auto-attendant 507

managing outbound line groups 481, 526, 528

manual key IPSec 373

marking 447

MD5 387

meet-me conference 532

Meet-me conference calls 547

memory usage 189, 190

message bar 52

Message Digest 5, see MD5

Message Waiting Indicator
- see MWI

messages
- CLI 54
- warning 52

metrics, see reports

Microsoft
- Challenge-Handshake Authentication Protocol (MSCHAP) 663
- Challenge-Handshake Authentication Protocol Version 2 (MSCHAP-V2) 663
- Point-to-Point Encryption (MPPE) 663

model name 187

MOH 532, 533
- file format 539
- overview 539

monitor

  ACD queue **219**
  BRI trunk **218**
  call recordings **222**
  CDR backup **223**
  CTI peer **216**
  FXO trunk **217**
  FXS peer **214**
  SA **211**
  SIP peer **213**
  SIP trunk **215**

monitor profile
  ADP **415**

Motion Picture Experts Group
  see MPEG

mounting
  rack **31**

MPEG **476**

MPPE (Microsoft Point-to-Point Encryption) **663**

MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) **663**

MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol Version 2) **663**

MSN **500**

MTU **256**

mu-law **470**

multiple SIP extensions, tutorial **138**

multiple slash encoding **425**

multi-slash-encoding attack **425**

Music On Hold
  see MOH

MWI **468**, **469**

My Certificates, see also certificates **646**

MySQL **722**

myZyXEL.com **229**
  accounts, creating **229**

N

NAT **299**, **323**
  address mapping, see policy routes
  ALG, see ALG
  and address objects **296**
  and address objects (HOST) **326**
  and ALG **335**, **336**
  and firewall **361**
  and interfaces **326**
  and policy routes **290**, **296**
  and to-Device firewall **327**
  and VoIP pass through **336**
  and VPN **390**
  and VPN, see also VPN
  configuration overview **100**
  limitations **299**
  loopback **328**
  port forwarding, see NAT
  port translation, see NAT
  port triggering **299**
  port triggering, see also policy routes
  prerequisites **100**
  traversal **390**
  trigger port, see also policy routes
  tutorial **129**

NBNS **244**, **266**, **273**, **278**

NetBIOS
  Broadcast over IPSec **373**
  Name Server, see NBNS.

NetMeeting **339**
  see also H.323

Network Address Translation, see NAT

network congestion **430**

network policy, see VPN connections

Network Terminal
  see NT mode

Network Time Protocol (NTP) **670**

nighttime call handling **595**

Nmap **421**

no answer forward **466**, **763**

No-IP **317**

non-RFC
  characters **425**
  defined-char attack **425**
  HTTP-delimiter attack **425**

NSSA **305**

NT mode **448**

O

object-based configuration **91**

objects **91**, **103**
  AAA server **631**

  addresses and address groups 613
  authentication method 639
  certificates 643
  for configuration 91
  introduction to 91
  schedules 625
  services and service groups 619
  users, user groups 599

obsolete-options attack 426

office hours 465, 595
  after hours 466, 763

One-Time Password (OTP) 632

Online Certificate Status Protocol (OCSP) 659
  vs CRL 659

Open Shortest Path First, see OSPF

operator, internal 433

order of feature application 94

OSPF 304
  and Ethernet interfaces 239
  and RIP 306
  and static routes 306
  and to-Device firewall 304
  area 0 305
  areas, see OSPF areas
  authentication method 239
  autonomous system (AS) 304
  backbone 305
  configuration steps 307
  direction 239
  link cost 239
  priority 239
  redistribute 306
  redistribute type (cost) 308
  routers, see OSPF routers
  virtual links 307
  vs RIP 302, 304

OSPF areas 304, 305
  and Ethernet interfaces 239
  backbone 305
  Not So Stubby Area (NSSA) 305
  stub areas 305
  types of 304

OSPF routers 305
  area border (ABR) 306
  autonomous system boundary (ASBR) 306
  backbone (BR) 306
  backup designated (BDR) 306
  designated (DR) 306
  internal (IR) 305
  link state advertisements
  priority 306
  types of 305

other documentation 2

OTP (One-Time Password) 632

outbound call routing 89

outbound line groups 88, 144, 150, 156, 477
  and LCRs 478
  BRI trunk 477
  codecs 486, 493
  FXO trunk 477
  LCRs 529
  management 481, 528
  SIP trunk 477
  trusted peer 477, 478
  types of 477

outgoing bandwidth 256

outgoing call restrictions 455

outside connections, types of 477

outside lines
  see outbound line groups

overlap 451

oversize
  chunk-encoding attack 425
  len attack 426
  offset attack 426
  request-uri-directory attack 426

P

packet
  flow 94
  statistics 196, 197

packet capture 739
  example 742
  files 738, 741, 743, 744
  troubleshooting 773

packet captures
  downloading files 738, 741, 744

packet capturing
  tutorial 171

packet forwarding 447

packet loss 430

page groups

  adding 550, 563
  editing 550, 563
PAP (Password Authentication Protocol) 663
parking lot extension 534
parking, call 532
Password Authentication Protocol (PAP) 663
PBX 27, 429
  ACD queue 219
  BRI trunk monitor 218
  call recording 764
  call recordings 222
  CTI peer 216
  FXO trunk monitor 217
  FXS peer monitor 214
  global setting 429
  packet capturing 171
  peer info 760
  SIP peer monitor 213
  SIP trunk monitor 215
  tutorials 135
  voice interfaces 448
PCM 475
Peanut Hull 317
peer IP PBX 37
Peer-to-peer (P2P)
  calls 125, 336
Perfect Forward Secrecy (PFS) 375
  Diffie-Hellman key group 392
performance
  troubleshooting 768
per-hop behavior 447
Personal Identification Number code, see PIN code
personal voice mail 584
PFS (Perfect Forward Secrecy) 375, 392
PHB 447
phonebook 587, 588, 591, 592, 759
physical ports
  and interfaces 92
  packet statistics 196, 197
picking up parked calls 532
PIN code 256
PIN generator 632
pipeline 447
playing voice mail 585
pointer record 675
Point-to-Point Protocol over Ethernet, see PPPoE.
Point-to-Point Tunneling Protocol, see PPTP
policy enforcement in IPSec 374
policy route
  troubleshooting 766
policy routes 290
  actions 291
  and address objects 295
  and ALG 336, 339
  and HTTP redirect 332
  and interfaces 296
  and NAT 290
  and schedules 295, 405, 407
  and service objects 620
  and trunks 281, 295
  and user groups 294, 295, 405, 407
  and users 294, 295, 405, 407
  and VoIP pass through 336
  and VPN connections 295, 770
  bandwidth management 297
  benefits 290
  BWM 292
  configuration overview 98
  criteria 291
  overriding direct routes 292
  prerequisites 99
pop-up windows 43
port forwarding, see NAT
port groups 107, 234, 236
port roles 236
  and Ethernet interfaces 236
  and physical ports 236
port scan, filtered 422
port scanning 421
port sweep 422
port translation, see NAT
port triggering 299
  and firewall 296, 768
  and policy routes 296
  and service groups 297
  and services 297
  troubleshooting 768
PostgreSQL 720, 721
power off 36, 755
power on 36
PPP 279
  troubleshooting 767
PPP interfaces

- subnet mask 276
- PPPoE 279
  - and RADIUS 279
  - TCP port 1723 279
- PPPoE/PPTP interfaces 234, 246
  - and ISP accounts 247, 661
  - basic characteristics 234
  - gateway 247
  - subnet mask 247
- PPTP 279
  - and GRE 279
  - as VPN 279
- precedence 447
- priority 431
- privileges 454
- problems 765
- product
  - overview 28
- product registration 856
- protocol anomaly 411, 425
  - detection 418
- proxy servers 331
  - web, see web proxy servers
- PSAP 532
- PSTN 27, 88, 478
  - connections to 143
- PSTN calls, tutorial 143
- PTR record 675
- Public Safety Answering Point
  - see PSAP
- public server tutorial 129
- Public Switched Telephone Network
  - see PSTN
- Public-Key Infrastructure (PKI) 644
- public-private key pairs 643
- Pulse Code Modulation
  - see PCM

Q

- QoS 290, 397, 430, 431, 440
- Quality of Service
  - see QoS
- quantization 475
- Quick Start Guide 2

R

- rack-mounting 31
- RADIUS 631, 633
  - advantages 631
  - and IKE SA 391
  - and PPPoE 279
  - and users 600
  - user attributes 611
- RADIUS server
  - troubleshooting 771
- Real Time Transport Protocol
  - see RTP
- realm 432
- Real-time Transport Protocol, see RTP
- reboot 36, 105, 753
  - vs reset 753
- record of calls 225, 227
- recording audio
  - files 516
- recording calls 544
- Reference Guide, CLI 2
- registration 229
  - configuration overview 98
  - IP telephones 140
  - prerequisites 98
  - product 856
- related documentation 2
- Relative Distinguished Name (RDN) 633, 634, 635, 636
- remote access IPSec 373
- Remote Authentication Dial-In User Service, see RADIUS
- remote management
  - configuration overview 104
  - FTP, see FTP
  - prerequisites 104
  - see also service control 678
  - Telnet 698
  - to-Device firewall 354
  - WWW, see WWW
- remote network 367
- replay detection 373

reports
  collecting data **201**
  configuration overview **105**
  daily **706**
  daily e-mail **706**
  specifications **203**
  traffic statistics **200**

representative number **484**
  SIP trunk **484**

reset **774**
  vs reboot **753**

RESET button **36**, **774**

restricting outgoing calls **455**

resuming parked calls **532**

RFC
  1058 (RIP) **302**
  1389 (RIP) **302**
  1587 (OSPF areas) **305**
  1631 (NAT) **299**
  1889 (RTP) **340**
  2131 (DHCP) **277**
  2132 (DHCP) **277**
  2328 (OSPF) **304**
  2402 (AH) **374**, **392**
  2406 (ESP) **374**, **392**
  2510 (Certificate Management Protocol or CMP) **650**
  2516 (PPPoE) **279**
  2637 (PPTP) **279**
  2890 (GRE) **279**

RFC 1889 **430**

RFC 2833 **469**, **470**

ring groups
  configuration **549**, **562**
  overview **549**

RIP **302**
  and Ethernet interfaces **238**
  and OSPF **303**
  and static routes **303**
  and to-Device firewall **303**
  authentication **303**
  direction **238**
  redistribute **303**
  RIP-2 broadcasting methods **238**
  versions **238**
  vs OSPF **302**

Rivest, Shamir and Adleman public-key algorithm (RSA) **649**

round robin **288**

routing
  troubleshooting **768**

Routing Information Protocol, see RIP

routing protocols **302**
  and authentication algorithms **312**
  and Ethernet interfaces **237**

routing, by SIP To header **486**, **493**

RSA **649**, **652**, **658**

RTP **340**, **430**, **431**
  DTMF **470**
  see also ALG **340**

RTP and DTMF **469**

S

sampling **475**

SCEP (Simple Certificate Enrollment Protocol) **650**

schedule
  troubleshooting **771**

schedules **625**
  and current date/time **625**
  and firewall **351**, **363**, **405**, **407**
  and policy routes **295**, **405**, **407**
  one-time **625**
  recurring **625**
  types of **625**
  where used **103**

screen resolution **43**

second call **532**

Secure Hash Algorithm, see SHA1

Secure Socket Layer, see SSL

security associations, see IPSec

security settings
  troubleshooting **766**

self-directory-traversal attack **426**

self-referential directories **426**

sensitivity level **417**

serial number **187**
  softphone **142**

service control **123**, **678**
  and to-Device firewall **678**
  and users **679**
  limitations **678**
  timeouts **678**

service groups 620
  and firewall 363
  and port triggering 297
  where used 103
service objects 619
  and firewall 620
  and IP protocols 620
  and policy routes 620
service subscription status 232
services 619, 827
  and firewall 363
  and port triggering 297
  where used 103
Session Initiation Protocol
  see SIP
session limits 355, 364
sessions 203
sessions usage 189, 191
SHA1 387
shell script
  troubleshooting 773
shell scripts 725
  and users 611
  downloading 734
  editing 733
  how applied 726
  managing 733
  not stopping or starting the device 36
  syntax 726
  uploading 735
shutdown 36, 755
signal quality 208, 209
SIM card 256
Simple Certificate Enrollment Protocol (SCEP) 650
Simple Network Management Protocol, see SNMP
simultaneous ringing 549
SIP 37, 336
  ALG 335
  and RTP 340
  authentication 137, 140
  DTMF 469, 470
  extensions 87, 136, 137
    adding 462
    configuring 136
  peers 469
  phone configuration 140
  realm 432
  registration 141
  server 38
    settings 431
  To header 486, 493
  trunk 150, 478, 484
    auto-attendant 486, 493
    caller ID 485, 492
    channel limit 484, 491
    codecs 486, 493
    settings 483, 490
SIP trunk monitor 215
smurf attack 423
SNAT 299
  troubleshooting 768
SNMP 700, 701
  agents 701
  and address groups 703
  and address objects 703
  and zones 703
  Get 701
  GetNext 701
  Manager 701
  managers 701
  MIB 701, 702
  network components 701
  Set 701
  Trap 701
  traps 702
  versions 700
snom 575
softphones 37
sound
  quality 430, 447, 475
Source Network Address Translation, see SNAT
spillover (for load balancing) 284
SQL (Structured Query Language) 721
SSH 693
  and address groups 696
  and address objects 696
  and certificates 696
  and zones 696
  client requirements 695
  encryption methods 695
  for secure Telnet 696
  how connection is established 694
  versions 695
  with Linux 697
  with Microsoft Windows 696

SSL 679
stac compression 663
starting the device 35, 36
startup-config.conf 731
  if errors 728
  missing at restart 728
  present at restart 728
startup-config-bad.conf 728
static DHCP 344
static routes 290
  and interfaces 298
  and OSPF 306
  and RIP 303
  configuration overview 99
  metric 299
  prerequisites 99
statistics
  daily e-mail report 706
  traffic 200
status 185
status bar 52
  warning message popup 52
stopping the device 35, 36
streaming video 476
stub area 305
subscription services
  status 232
  upgrading 232
supported browsers 43
SWM 292
SYN flood 424
syslog 709, 716
syslog servers, see also logs
system log, see logs
system name 187, 666
system reports, see reports
system uptime 187
system-default.conf 731

T

T/TCP 426
TAPI 431, 442
  CTI client 431
  driver 431
  driver installation 443
  example 431
  software 431
target market 28
TCP 619
  ACK (acknowledgment) 423
  connections 619
  decoder 418, 425
  decoy portscan 422
  distributed portscan 422
  port numbers 619
  portscan 421
  portsweep 422
  RST 422
  SYN (synchronize) 423
  SYN flood 423
TE mode 448
technical reference 183
TEI 451
telephone adapter, analog
  see ATA
telephone exchange device 27
Telnet 698
  and address groups 699
  and address objects 699
  and zones 699
  with SSH 696
Terminal Endpoint Identifier
  see TEI
Terminal Equipment
  see ISDN TE mode
terminology 94
terms explained 87
text file 587
three-way handshake 424
throughput rate
  troubleshooting 772
time 667
time servers (default) 670
time-based auto-attendant configuration 595
time-critical applications 430
To header, routing by 486, 493
to-Device firewall 354
  and NAT 327
  and NAT traversal (VPN) 770

  and OSPF 304
  and remote management 354
  and RIP 303
  and service control 678
  and VPN 770
  global rules 354
  see also firewall 354

token 632

tones 470

trademarks 855

traditional PBX 478

traffic
  forwarding 447
  marking 447

traffic anomaly 411, 415

traffic statistics 200

transferring call settings 542

Transmission Control Protocol, see TCP

transport encapsulation 374

Transport Layer Security (TLS) 700

triangle routes 360
  allowing through the firewall 361
  vs virtual interfaces 360

Triple Data Encryption Standard, see 3DES

troubleshooting 737, 742, 765
  admin user 771
  bandwidth limit 768
  cellular 767
  certificate 771
  configuration file 773
  connection resets 769
  DDNS 768
  device access 765
  ext-user 771
  firewall 766
  firmware upload 773
  HTTP redirect 769
  interface 766
  Internet access 766, 770
  IPSec VPN 769
  LEDs 765
  logo 772
  logs 772
  management access 772
  packet capture 773
  packet flow 94
  performance 768
  policy route 766
  port triggering 768
  PPP 767
  RADIUS server 771
  routing 768
  schedules 771
  security settings 766
  shell scripts 773
  SNAT 768
  throughput rate 772
  VLAN 768
  VPN 770

truncated-address-header attack 427

truncated-header attack 426, 427

truncated-options attack 426

truncated-timestamp-header attack 427

trunk 477

trunks 234, 281, 477
  and ALG 339
  and policy routes 281, 295
  configuration overview 98
  member interface mode 288
  member interfaces 288
  prerequisites 98
  see also load balancing 281
  tutorial 111
  where used 98

Trusted Certificates, see also certificates 654

trusted peer 88, 478
  representative number 492

TTCP-detected attack 426

tunnel encapsulation 374

tutorials 107, 135
  authority group 137
  auto provisioning 141
  configure SIP extensions 136
  dial conditions 145, 157
  feature codes 163
  internal calls 136
  IP telephones 140
  ISDN calls 154
  ISDN network configuration 159
  ITSP calls 147
  ITSP connection 148
  LCRs 144, 151, 156
  multiple SIP extensions 138
  overview 135
  packet capturing 171
  PSTN calls 143

U

UDP 619
  decoder 418, 425
  decoy portscan 422
  distributed portscan 422
  flood attack 424
  messages 619
  port numbers 619
  portscan 421
  portsweep 422
u-encoding attack 426
u-law 470
undersize-len attack 426
undersize-offset attack 426
unreachables (ICMP) 422
upgrading
  firmware 731
  licenses 232
uploading
  configuration files 731
  firmware 731
  shell scripts 733
usage
  CPU 189, 190
  flash 189
  memory 189, 190
  onboard flash 189
  sessions 189, 191
user authentication 599
  external 600
  local user database 632
user awareness 601
User Datagram Protocol, see UDP
user group objects 599
user groups 599, 600
  and firewall 363, 366
  and policy routes 294, 295, 405, 407
  configuration overview 104
user name
  rules 602
user objects 599
user sessions, see sessions
User’s Guide 25
user-aware 116
users 599
  access, see also access users
  admin (type) 599
  admin, see also admin users
  and AAA servers 600
  and authentication method objects 600
  and firewall 363, 366
  and LDAP 600
  and policy routes 294, 295, 405, 407
  and RADIUS 600
  and service control 679
  and shell scripts 611
  attributes for Ext-User 600
  attributes for LDAP 610
  attributes for RADIUS 611
  attributes in AAA servers 610
  configuration overview 104
  currently logged in 188, 193
  default lease time 607, 609
  default reauthentication time 607, 609
  default type for Ext-User 600
  ext-group-user (type) 599
  Ext-User (type) 600
  ext-user (type) 599
  groups, see user groups
  Guest (type) 599
  lease time 603
  limited-admin (type) 599
  lockout 608
  prerequisites for force user authentication policies 104
  reauthentication time 603
  types of 599
  user (type) 599
  user names 602
UTF-8 decode 426
UTF-8-encoding attack 426

V

Vantage Report (VRPT) 709, 716
video codecs 468, 470, 475
virtual interfaces 234
  basic characteristics 234
  not DHCP clients 276
  vs asymmetrical routes 360
  vs triangle routes 360
Virtual Local Area Network, see VLAN.

Virtual Private Network, see VPN
VLAN 259
  advantages 260
  and MAC address 260
  ID 260
  troubleshooting 768
VLAN interfaces 234, 260
  and Ethernet interfaces 261, 768
  basic characteristics 234
vocal synthesizer 475
voice codecs 468, 470, 475
voice coder/decoder 468
voice interfaces 448
voice mail 38, 433, 467, 581, 582
  authentication 583
  change folder 585
  email notifications 38
  feature code 163
  forwarding 462, 581
  listening to messages 585
  mail box options 586
  message stored capability 586
  personal 584
  settings 763
voice mail forwarding 462
voice mal
  accessing 583
Voice over Internet Protocol
  see VoIP 37
VoIP 37
  account example 148
  and emergency calls 532
  gateways 37
  interconnected 532
VoIP pass through 339
  and firewall 336
  and NAT 336
  and policy routes 336
  see also ALG 335
VPN 367
  active protocol 392
  and NAT 390
  and the firewall 355
  basic troubleshooting 769
  IKE SA, see IKE SA
  IPSec 367
  IPSec SA
  proposal 387
  security associations (SA) 368
  see also IKE SA
  see also IPSec 367
  see also IPSec SA
  status 192
  troubleshooting 770
VPN connections
  and address objects 370
  and policy routes 295, 770
VPN gateways
  and certificates 370
  and extended authentication 370
  and interfaces 370
  and to-Device firewall 770
VRPT (Vantage Report) 709, 716

W

warm start 36
warning message popup 52
warranty 855
  note 855
Web Configurator 35, 43
  access 43
  access users 609
  requirements 43
  supported browsers 43
web phone 757
  phonebook 759
web proxy servers 332
  see also HTTP redirect
webroot-directory-traversal attack 426
weighted round robin (for load balancing) 283
white list 462, 761
Windows Internet Naming Service, see WINS
Windows Internet Naming Service, see WINS.
WINS 244, 266, 273, 278
WINS server 244
Wizard Setup 59, 69
WWW 680
  and address groups 683
  and address objects 683
  and authentication method objects 682
  and certificates 681
  and zones 683

  see also HTTP, HTTPS 123, 680

Z

zones 92, 313
  and firewall 354, 362
  and FTP 700
  and interfaces 92, 313
  and SNMP 703
  and SSH 696
  and Telnet 699
  and VPN 92, 313
  and WWW 683
  block intra-zone traffic 316, 361
  configuration overview 99
  default 93
  extra-zone traffic 314
  inter-zone traffic 314
  intra-zone traffic 314
  prerequisites 100
  types of traffic 313
  where used 100

µ-law 470, 475